# Resisting Securitization

## Analysing the discourse of resistance used by opposers of the Law on Intelligence- and Security Services

**Martijn Harkema**

s1501704

Master's Thesis Crisis and Security Management

Supervisor: Dr. Tommy van Steen

Second Reader: Dr. Tatiana Tropina

7 June 2020

15624 words

**Abstract**

On the 21st of March, 2018, a referendum was held on the new Dutch Law on the Intelligence- and Security Services (WIV). The debate on this law was inseparable from the debate on terrorism and was thus to a large extent securitized, which provided difficulties for opposers of this new law. Literature shows that resistance against securitization is possible by making use of one or more resistance strategies. The first strategy is desecuritization, which means to take a topic out of the realm of security. Secondly, there's counter-securitization, meaning the positioning of another security threat against the threat that is framed by a government. The third is delegitimization, a strategy which targets the legitimacy of a security measure. This research is aimed at finding out which of these tactics were used by the opposers of the WIV.

This study does a discourse analysis of sources that were published by actors opposing the WIV. The main findings of the study are (1) that desecuritizing strategies were not used by any actors, probably because terrorism is accepted by all actors as a security problem. (2) Counter-securitization was used as a resistance tactic by various actors. It was notable that all of these actors were located at the political flanks, both left and right. Lastly (3), delegitimizing strategies were used mostly on the political flanks, but were also used by a few actors located in the political centre. The implications of these findings are that counter-securitization theory does not only apply to conflict situations, but also to normal political debates, and that delegitimization strategies can be targeted not only at security measures, but also at the actors implementing them. Future research should be done on the effectiveness of resistance tactics by analysing the response of the audience to such discourses.

## Contents

## Introduction

On the 21st of March, 2018, an advisory referendum was held in the Netherlands, concerning the Law on the Intelligence- and Security Services (WIV). After fierce debates on the law, both in official parliamentary debates as well as in popular media, the referendum ended in a defeat for the government, with 46% of people voting in favour of the law, and 49% against (Kiesraad 2018). The WIV is a law that is intended to give the Services broader possibilities to track the online behaviour of citizens that are suspected of terrorist behaviour. According to the government, new legislation was needed because the legal framework the services had to operate in was outdated, because of which they were not able to operate effectively. (Ollongren, 2017) While opposers of the law did not disagree that existing legislation at the time was indeed outdated, they thought that the amount of freedom that the services would get to operate was too big, and that there needed to be more checks and balances in place to make sure the services would not violate the privacy of citizens. The main feature of the law that caused resistance was the part allowing for 'fishing expeditions', which are mass data collection operations, which, apart from the data from potential suspects, also catch the data of large numbers of innocent citizens. Other arguments are the long period of time in which the services can retain data, and the freedom of services to share these data with foreign intelligence services (Bolwijn, 2018). The people opposing the WIV called this part of the law the *Sleepnet*, which caused the referendum on the WIV to be called *Sleepnet-referendum* in popular discourse.

The debate around the WIV has to be interpreted in the context of a much larger debate about security and privacy violations. Since 9/11, counterterrorism policies in the US and Europe have radically changed, and the intelligence agencies have received more and more freedom to use surveillance tactics to keep their countries safe from terrorist threats (Babu-Kurra, 2011). While some of these strategies are very efficient to keep an eye on individual suspects, other strategies, such as 'fishing expeditions', have been criticized for infringing the privacy of a the public. In the decade after 9/11, the public either was not aware of the fact that intelligence agencies were expanding their capabilities to spy on the people, or simply did not care about this, preferring security over privacy. This changed, however, with the revelations done by whistle-blower Edward Snowden in 2013, in which it was confirmed that large-scale digital surveillance techniques were frequently used by the NSA. (MacAskill and Dance, 2013). As people got more aware of the negative consequences of increased security, the

opposition against counter-terrorism legislation started to grow, and the results of the WIV referendum are a clear example of this.

This thesis project will research the debate surrounding this referendum, especially the discourse used by those actors opposing the WIV. When arguing in favour of increasing surveillance capacities of intelligence services, governments usually use language of security, thereby securitizing the potential threat of terrorists and thereby allowing themselves to impose emergency measures (De Graaf, 2011, amongst others). Usually, choosing this tactic of securitization makes it quite easy for governments to convince the public of the necessity of certain measures. On the other side of the debate, opposers of these measures will generally have difficulties resisting this securitization, but looking solely at the referendum results, the opposers in this case have managed to. This is what makes researching the opposing discourse so interesting. What this thesis aims to find out is what kind of tactics the opposers of such measures used in their discourse in order to provide resistance against these securitizing tactics. The research question this thesis tries to answer is ***What tactics of resistance have been used by the opposers of the WIV against the securitizing discourse used by the proponents of this law?*** The method used in order to find an answer to this question is discourse analysis. The research will analyse a wide range of sources, from political debates to opinion articles and tv programmes.

*Relevance*

Finding an answer to this question is relevant for the academic world and for society. First, this study uses a conceptual framework based on the theory of counter-securitization. This is a relatively new theory which, though it has been mentioned since the introduction of securitization theory (Buzan, Weaver, De Wilde, 1998), has not been explained much further until 2015 (Stritzel and Chang, 2015). Stritzel and Chang used the theory to study a case of military conflict. Vuori (2015) and Topgyal (2016) applied the concept to a non-traditional security issue, but both case studies were situated in China, a nondemocratic state, so the situation was incomparable. This paper can thus add to counter-securitization theory, by applying the framework to a debate in a democratic society. Furthermore, while several authors have dedicated articles to securitization of terrorist threats in order to implement counterterrorism policies (See e.g. De Graaf and Eijkman, 2011), no research has been done about the discourse used by opposers of such legislation. This thesis could fill this gap in the literature.

The study is relevant for society since it analyses one of the larger debates that has taken place recently in the Netherlands. The WIV referendum has received a large amount of media coverage, and over half of the electorate (51,54%) turned up to vote, illustrating that is was a topic that received the attention of a very large group of people (Kiesraad, 2018). Apart from the fact that this thesis researches such a relevant debate, the outcomes of this research project might be useful for actors participating in further debates, because it could provide them with strategic insights on how to resist securitizing discourse. This is important because an issue being securitized is usually not seen as advantageous for the openness of the debate surrounding the topic. If possible, issues are almost always better dealt with in the ordinary public sphere. (Buzan, Weaver, De Wilde 1998)

## Context

*Background*

As mentioned in the introduction, the *WIV-referendum, Sleepwet-referendum* (as it was called by a large part of the media, as a result of framing by the opposers of the law), or officially *referendum on the law on the intelligence- and security services 2017*[1] was held on the 21st of March, 2018. This date was chosen for logistical reasons, as it would coincide with municipal elections in a large part of the Netherlands.

The WIV-referendum was a consultative referendum. This means that the government was not obliged to take action according to the result of the referendum. In fact, the leader of government party CDA, Sybrand van Haersma Buma, months before the referendum, already made clear the government would ignore the outcome of the referendum, as he thought the WIV was absolutely necessary (Meijer and Hendrickx, 28 Oct 2017). This remark might have had quite an influence on voters. As Meijer and Hendrickx write, this means the referendum has become 'pointless', and voters might thus be discouraged to vote. On the other hand, the remark can also create an extra motivation for voters, who feel like the way Buma acts is unacceptable (Paternotte, 29 Oct 2017).

This referendum was the second consultative referendum that was held in the Netherlands, after the referendum on the EU-Ukraine association treaty. Furthermore, it was also the last consultative referendum (for now), since the law that facilitates such referenda was revoked, already before the 21st of March 2018.

*Initiation of the referendum*

The referendum was initiated by five students form Amsterdam, who started a 'citizen's initiative'[2] to collect signatures. 300.000 signatures were necessary for the referendum to go through, and this number was reached by 9 October 2017 (Van der Leeuw, 2018). The initiative was endorsed by NGO's and media like Amnesty International, GeenStijl, the Dutch Association of Journalists (NVJ), Free Press Unlimited and Bits of Freedom. Because of these endorsements the first wave of publicity was generated, and the initiative managed to reach 10.000 signatures. However, it wasn't until Arjen Lubach, in his influential TV-show Zondag met Lubach, called on his public to sign the petition for a referendum, that it got massive attention. (Jacobs et al. 2018)  As often goes with the subjects Lubach talks about, the WIV

[1] Referendum over de wet inlichtingen- en veiligheidsdiensten 2017
[2] Burgerinitiatief

became a topic many people talked about, and a week after the broadcast, the threshold was reached.

*Results and figures*

46% of the people who turned up voted in favour of the new WIV, while 49% voted against. The total turnout for the referendum was 51.5% (Kiesraad 2018). People who voted against mainly lived in the north of the Netherlands and in the large cities. Women were a little more likely to vote against the WIV than men, and younger people were more likely to vote against then older people.

(NOS.NL) – RED = MUNICIPALITIES IN WHICH THE MAJORITY VOTED AGAINST THE WIV. BLUE = MUNICIPALITIES IN WHICH THE MAJORITY VOTED IN FAVOUR OF THE WIV

The main reasons to vote in favour of the new WIV were that people thought it was necessary to protect our security (58%), that they had 'nothing to hide' (13,7%), or that the WIV was in need of modernisation (4,5%). The main reasons to vote against the new WIV were that the new law damages privacy too badly (38,8%), the law isn't good in its current form (12,2%), data can end up abroad (10%), people do not trust politicians (6,6%), or too few safeguards (4,8%). The opinion that the WIV damages the privacy of citizens is shared by 38,4% of the whole electorate, while over 80% of those who voted against think this is the case (Jacobs et al. 2018).

The fact that younger people mainly voted against the WIV rhymes with the fact that the large cities and university cities all voted against the WIV, as they generally have younger populations with a large amount of students. Furthermore, large cities generally vote more left-wing than rural areas. The north of the Netherlands does not have a particularly young population, but is generally known to be 'red'. This, however, is not the only thing that explains the fact that this part of the country voted so massively against the WIV.

In the North, and especially in the Groningen province, there is a high amount of distrust in 'The Hague': the government and political parties. To a large extent, this can be seen as a result of the problems in this region with the gas extraction and the subsequent earthquakes

happening there. Another reason named for this distrust is simply the distance between the north and The Hague (Altena and van Atteveld, 22 March 2018).

When looking at the political parties that voters support, we see that three quarters of the voters of GroenLinks and SP voted against the WIV, while over two-thirds of the voters of government parties VVD and CDA voted in favour. This is in line with the viewpoints of these parties. Only with D66, a party that was against the WIV before it joined the government coalition, and PVV, a party that was in favour of the WIV but generally attracts a lot of protest voters, we see that the party line and the choice of their voters do not align. (Schellevis and Herderschee, 22 March 2018).

## Theory

### *Security and Securitization*

Since the end of the Cold War, the concept of security has been subject to changes to the way it is defined. In the bipolar world that existed during the times of the Cold War, the dominant definition of security was the definition provided by realism. Kenneth Waltz (1979) describes security as a matter that is mainly concerned with the survival of states. Security, therefore, is traditionally seen in the context of national security, from a pure military perspective. As, the Cold War ended, however, and the survival of the two superpowers and their allies was no longer the main topic of research in security studies, scholars started to realise that this conception of security was no longer sufficient. Therefore, new approaches to the concept of security were introduced.

One of these new approaches is the theory of securitization by the Copenhagen School. This school of thought states that there are no objective threats waiting to be discovered. Instead, we create our own threats and security matters through discourse (Trombetta 2008). Depending on the discourse surrounding a certain topics, these topics can be anywhere between non-politicized, meaning that politicians and the state do not deal with the topics, to politicized, meaning that the topic is part of political debate and government policy, to securitized, meaning the topic is generally conceived as an existential threat to society (Buzan, Waever, De Wilde 1998, p.23). If an issue has been securitized, this means there is the general conception that emergency measures are necessary to protect society or the state against this threat. Such emergency measures can be taken outside the bounds of political procedure. Issues can both be securitized by the state as well as by other actors, such as the media, politicians or society as a whole. Also, topics that can be securitized are very variate. Examples are culture, religion, the economy and the environment.

A certain subject being securitized is preceded by a securitizing move: A discourse that takes the form as presenting something as an existential threat (Buzan et al., p.25). Whether such a move succeeds is dependent on three factors. The first factor is whether the speech act follows the ‘grammar of security’, which means that the speech act should present the issue as an existential threat, with a point of no return and a possible way out. (Buzan et al.), or that, as explained by Stritzel (2014), the securitizing language should contain a claim, a warning, a demand and supporting evidence of the claims. Furthermore, the relationship between the securitizing actor and the public is important. The securitizing actor should have enough social capital to be able to influence the public with its rhetoric, meaning that the actor should

be in a position of authority (not necessarily meaning it has to be an official authority / state actor). Thirdly, the alleged threat should take a concrete form so that he public can recognise the issue as a threat. (Buzan et al., p.33)

Apart from fulfilling the above requirements, a securitizing move also needs to find an 'empowering audience', that has a direct causal connection with the issue and that has the ability to enable the securitizing actor to take the measures that are considered necessary to tackle the perceived threat (Balzacq 2010, p.9). The support for a securitizing move from an audience can come in the form of moral support, meaning the public generally supports a certain action against a threat, and formal support, coming from the respective legislative body that should give the securitizing actor formal permission to adopt a certain policy. Only when a securitizing move sufficiently meets the requirements for its discourse, as well as the right audience, it will lead to a successful securitization. Otherwise, it will remain simply a securitizing move, or failed securitization.

*Resistance against securitization: Desecuritization, counter-securitization and delegitimization*

While certain issues can move into the sphere of security, simultaneously other issues move back out from this sphere. Issues of security can be moved out of this sphere by people or groups opposing a certain securitizing move through resistance. Stritzel and Chang (2015, p.553), have created a typology of resistance against securitizing moves, and in this typology they describe three forms in which this resistance can exist: desecuritization, counter-securitization and delegitimization. In this chapter, we will go through all three of them, starting with desecuritization. Desecuritization is the process by which security threats lose their status as such. According to Buzan, Waever and De Wilde (1998), desecuritization is the optimal long-range option, since it sees securitization as a negative and prefers issues to be dealt with in the ordinary public sphere.

Hansen (2012) describes four ways in which the process of desecuritization can take place. First, the process can happen in silence; as a certain issue starts to become less threatening to society – for whatever reason – it will lose its status as a matter of security. Second is desecuritization through replacement. In this strategy, one issue is taken out of the security realm while another is simultaneously securitized. Hansen quotes Behnke (2006), who theorises that people will always find something that they interpret as threatening to them, and

that an issue cannot be desecuritized without another issue being securitized. Third, there is desecuritization by rearticulation. This strategy aims to desecuritize an issue by actually solving the issue: when a certain threat is removed, and the problem does thus not exist anymore, it is of course not a security problem anymore. This approach appear straightforward, however, with most security issues it is of course easier said than done to actually resolve the security problem. Fourth, Hansen also names desecuritization through stabilisation, which is, like silencing, not an active strategy, but it is a way in which issues can move out of the security realm. When a threat has been looming for a long time, and there is no perspective of resolving the issue, the threat slowly move out of the security realm, while it actually continues to loom. (Hansen, 2012)

Vuori (2011) names another strategy for desecuritization, which is used by groups of actors that are the referent object of securitization strategies by the state to resist this securitizing move. He writes that when a certain group is framed as a threat to certain values, this group can turn the discourse around by framing themselves, and their activities, as contributing to these values, and not against them. In other words, the group tries to give itself a positive image to fight the negative discourse spread by the state. (Vuori 2011, p.192) Important to notice is that when using this strategy, the discourse of the group that is being securitized, is explicitly not aimed at criticizing the securitizing actor; the discourse is only aimed self-description and thus giving the group itself a better reputation without actively damaging the reputation of the securitizing actor. (Vuori 2011, p.200)

If the target group does not manage to stop the process of securitization by these means, the strategy of counter-securitization can be used. Though the concept of counter-securitization has been briefly mentioned in the works of Buzan et al. (1998) and Vuori (2011), it has not been explained in detail until 2015. Vuori (2011, 2015), in his case studies on social movements in China, described this transitioning process from desecuritization to counter-securitization. One of the case studies is about the Falungong movement, a religious and spiritual movement active since the 1990s. While in the beginning of its existence tolerated by the Communist Party of China, this changed in 1999. In order to be able to ‘legitimately’ suppress the FLG, the Party resorted to securitizing rhetoric. The FLG first tried to resist this by desecuritizing itself, by spreading discourse that was aimed at improving their own reputation. As this turned out to fail, the FLG changed strategy, choosing for a discourse that framed the Party as an existential threat to their community. While the FLG did not manage to legitimise itself by changing public opinion in its favour (which is logical given the situation;

it is hard to fight the propaganda machine that is the Chinese government), Vuori did provide a good example of how counter-securitizing tactics are used. What he did not do yet, though, is create a clear definition of the concept.

According to Stritzel and Chang (2015), counter-securitization is a form resistance against a securitizing move. This resistance can come from the group that is the target of a securitizing move, as illustrated by Vuori (2011, 2015), but this does not have to be the case. It can also come from a group that was not directly targeted by the securitizing actor, but that was nonetheless negatively affected by the emergency measures (Topgyal 2016), or a third actor that is engaged with the fate of the target group. Stritzel and Chang define "counter-securitizing moves resisting crucial elements of the securitization process […] as indeed counter-securitizing in the sense that *counter-securitizing moves also follow the ideal-type of the grammar of securitizing speech acts of claim, warning, directive and propositional content*" (emphasis added) (2015, p.552). In other words, a counter-securitizing move is a move that resists securitization by using the same grammar of security.

Stritzel and Chang use a case study of securitization during the Afghan war to support their theory. However, this does not mean that the theory is only applicable to situations of military conflict. Topgyal (2016, p.169) writes that "non-traditional security issues are just as interactive and open to counter-securitization", which he confirms by analysing a case study of Tibetan resistance against repression by the Chinese government. As a part of this resistance, at least 155 Tibetans self-immolated since 2009. Topgyal identifies these self-immolations as a counter-securitizing move against the Chinese securitizing discourse, aimed at the Tibetan people. From this case, Topgyal draws two more important theoretical conclusions, namely that a securitizing and counter-securitizing move can have the same audience, and that a counter-securitizing move is not necessarily a literal 'speech act', but that it can also be an 'act of speech', or symbolic act, such as the self-immolations in the case study.

Next to desecuritization and counter-securitization, Stritzel and Chang (2015) name a third method of resistance against securitization, namely delegitimization. Delegitimization is similar to counter-securitization in the sense that it involves a speech act intended to erode the legitimacy of the securitizing actor (Stritzel and Chang 2015, p.552). Counter-securitization, does so specifically by using the grammar of security, while delegitimization can include other tactics. The problem with Stritzel and Chang's explanation of this method is that they fail to properly define this it (Olesker 2018, p.313). The first step to get a good overview of

what delegitimization could entail is to find out what role legitimacy plays in securitization theory. A definition by Balzacq (2019) is used for this.

Balzacq (2015a, p.3) writes that "security practices draw their efficacy from legitimacy". As long as security practices are deemed legitimate, they will not be contested. The erosion of security practices' legitimacy would thus increase the chances of contestation, and it is possible to resort to legitimacy in the process of resistance (ibid, p.4).

Legitimacy, according to Balzacq (2019) consists of three main features: legality, justification and consent. An emergency measure imposed by a securitizing actor must conform to these three features in order to be accepted by the audience as legitimate. The principle of legality means that a measure, in order to be perceived as legitimate, must conform to the legal rules of a political system. Most democratic societies have strongly formalized legal systems, meaning that a government cannot simply change the rules in order to make its actions legitimate (ibid, p.345). The sheer fact that a certain measure is legal, though, does not mean that it is legitimate as well. It also has to be justified: the public has to be persuaded that the measure "contributes in a credible way to the achievement of society's values" (Coicaud 1997, p.23, as cited in Balzacq 2019, p.346), and a measure must be based on the shared norms and values of a political community (Gilley 2009, p.6). Lastly, measures are only legitimate if they enjoy the consent of the general public. This consent gives the government the right to develop policies to protect the object giving its consent (Balzacq 2019, p.346).

Since the literature on legitimacy and securitization does not explain clearly how a certain measure can be justified or not, this research makes use of some additional literature on proportionality. Macnish (2015) writes on the proportionality of surveillance operations, and defines the concept as "the harms of a particular act not outweighing the benefits of this act" (p.532). Different views exist on whether a certain harm does or doesn't outweigh a certain benefit, which means that proportionality is an issue that is almost always disputable. Furthermore, proportionality is a concept that is often used when assessing whether a certain surveillance operation is legitimate or not (Van Brakel and De Hert 2011). Since the concept is often used in debates on surveillance, I expect it to be used in the debates on the WIV-referendum as well. Arguments of disproportionality will be seen as de-justifying since a disproportionate measure cannot be seen as a measure that contributes in a *credible* way to the achievement of society's values.

*Assumptions*

This research makes two important assumptions that justify the research design in general, and more specifically the use of counter-securitization as a theoretical basis. The first of these assumptions is that authorities indeed make use of securitizing tactics in order to legitimately implement their counterterrorism policies. In academic literature, there are many articles that focus on government counterterrorism strategies, and more specifically on the discourse that comes with the implementation of such strategies, and these articles affirm the assumption that authorities have securitized terrorist threats.

De Graaf and Eijkman (2011) state that the 'referent object', or the threat, and the 'referent subject', or the one being threatened, have been broadened as a consequence of the securitisation of (Islamist) terrorism. As a consequence of this broadening, authorities have been able to legitimize the fact that the scope of counterterrorism policies has also substantially broadened, not only targeting very probable terrorist suspects, but virtually the whole population. This comment is also relevant to assess the probability of counter-securitization happening, as it states that this government discourse has broadened the referent subject from only the terrorists to the whole population. As the whole population is targeted by counterterrorism policies, it is more likely that the population will resist such a discourse.

Fisher (2011) writes that the development of an official discourse since 9/11 and the 7/7 London underground attacks, including terms such as international terrorism, helped the government change temporary emergency responses into permanent counterterrorism legislation. Furthermore, Kaunert and Leonard (2019) write about the securitization of terrorism on the European level, which has enabled governments to implement strong European counterterrorism networks. Croft (2012) and Pilecki et al. (2014) write about how exactly (Islamist) terrorism has been framed since 9/11, and they discovered the use of terms such as 'existential threat' or 'a threat transcending national interest'.

The second assumption is that the opponents of privacy-violating counterterrorism measures do indeed see such measures as a security issue. Pantazis and Pemberton (2013) confirm this assumption by describing three frameworks that have been used by groups resisting the advance of the security state in the United Kingdom, being human rights, liberty and freedom, and the criminalization of Muslim communities. Marx (2015) also writes that resistance against government surveillance is already happening on a large scale. He names various examples of ways in which people resist surveillance, tough these are all examples of strategies used by individuals.

Lamer (2017) describes the growing surveillance powers of the states as a consequence of the securitising of terrorist threats by the state. She then continues her argument by writing that increased surveillance powers by the state form a threat to freedom and human rights. In order to protect our freedoms and human rights, this securitising movement thus has to be stopped. She does not write about the ways in which this objective can be reached, but that further research should find out in which ways the narratives of securitisation can be countered.

Next to Lamer, there is a wide range of other authors that, in their work, share their concerns over the effects of counterterrorism policies on privacy, data protection and human rights. Amongst them are Chalk (1998), Dragu (2011), Engelmann (2012) and Richards (2013), the title of who's article illustrates the point clearly, being "The Dangers of Surveillance".

*Expectations*

Being an inductive research project, that tries to draw lessons from empirical observations instead of testing a theory, no clear hypothesis can be drawn from the theoretical framework. Nonetheless, on the basis of this framework, it can be expected that at least part of the discourse coming from the opposers of the WIV will include desecuritizing, counter-securitizing or delegitimizing language. This is because, following the logic of Buzan et al. (1998), the government, having securitized terrorist threats, logically would be able to implement their counterterrorism policies uncontested. The fact that the law was denied by the public in a referendum means that the terrorist threat has, at least to some extent, been brought out of the realm of security.

## Methodology

In order to understand the discourse surrounding the 21 March referendum, this thesis makes, perhaps not surprisingly, use of discourse analysis. Discourse analysis focuses on the use of language within a social context (Miles 2010, p.368). The most common way in which discourse materializes text. By text is not only understood written text or spoken words, but it can also exist in the form of certain images, acts or symbols (Balzacq, 2011). Examples of this are the self-immolations in Tibet as referred to by Topgyal (2016), or propaganda posters.

In securitization studies, researches mostly use critical discourse analysis. In general, this form of discourse analysis uses a broad body of data including, for example, interviews, pictures, archival materials and newspaper articles(etc.) Balzacq writes that this method of discourse analysis comes with one great advantage namely that "it offers a 'thick description' of the social practices associated with the construction and evolutions of threat images." (Balzacq, 2011b, p.41) When doing a discourse analysis, it is important to understand the features of a single text (what kind of actions does the text want to achieve?), as well as the relationship of this text with other texts in the debate, as a discourse is formed by multiple sources, and a single source should always be interpreted in the context of the wider debate around it (Hansen 2006).

### *A framework for discourse analysis*

In order to produce a sound discourse analysis, it is important to establish a framework which beacons the sources that can be used. This framework is established using Hansen's (2006) categorization of sources for discourse analysis. The first step is to choose an intertextual model: Official discourse, the wider political debate, popular/high culture and marginal discourse. For this study, the wider political debate will be analysed, which includes sources like political texts, parliamentary debates, editorials and columns, debates and opinions shared in TV programmes, political campaigns and contributions to NGOs. The choice to research the wider debate has been made because people base their political opinion on a large amount of sources dealing with the topic, and not only on official debates. Second, the amount of 'selves' studied has to be determined. In this case, these 'selves' are the actors contributing to the debate opposing the WIV. The exact number of actors featuring in this study is 28. Third is the temporal perspective. The material that is eligible for analysis has been produced between 28 October 2016 (Tweede Kamer, 2016), the date the WIV was proposed by the cabinet, and 21 March 2018, the date of the referendum. The debate around the WIV

intensified at two points during this temporal span, namely around the time the necessary signatures for the referendum were being collected (September – October 2017), and in the weeks preceding the referendum (1 March – 21 March). The vast majority of articles come from these two time periods. The sources that will be consulted will thus not be evenly spread over the larger time period. Fourth is the amount of events that are being researched. As this research is focused solely on the referendum of 21 March, the number of events is one.

*Data collection*

Data will be collected through various ways. First, a lot of information can be found on the internet. (Fragments of) TV programmes can be found on websites such as NPO Start or YouTube and statements by NGOs and political parties on their own websites. Furthermore, articles from newspapers can be accessed through Nexis Uni. From every actor, one or two relevant article will be chosen for analysis. This depends on the amount of relevant articles that are available for each actor. When an actor has only written or spoken once about the WIV referendum, this source will be analysed. When there are two or more relevant articles available, two articles are chosen. In the case of political parties, often a long article and a shorter campaign videos are chosen. In the case of (online) media outlets, two articles will be chosen randomly from all articles that dealt with the WIV referendum. The only opinion maker of which three sources will be analysed is Arjen Lubach, because of the large influence he had on the public, both when signatures were being collected and when the referendum took place.

Next, the data that will be collected will be organized in three categories. The first category is political discourse. By this is meant all contributions to the debate coming from politicians, or official spokespersons of political parties. The contributions can come from parliamentary debates, political parties' websites, appearances of politicians in tv shows or contributions of politicians to written media. The second category is interest groups and NGOs. By this is meant all official statements from NGOs or interest groups, or media appearances of official spokespersons of such organizations. The third category is opinion makers. This includes contributions to the debate made by people that is not a part of group 1 or 2. These contributions can appear in the form of contributions to written media, tv shows, or interviews. When collecting sources, attention will be given to the amount of authority a certain actor has. The public that a certain actor reaches is important to assess the weight of a certain contribution to the debate. Though it is difficult to assess exactly how much authority

a certain actor is, it is possible to estimate how many people have read or seen a certain source, for example by looking at audience ratings or subscription numbers.

*Data Analysis*

The first part of the data analysis will deal with the arguments that have been used by the actors opposing the WIV. The different kinds of arguments, dealing with for example privacy, efficacy, journalists, etc., will be summed up and examples of them will be given to create a good overview of which points the opposers of the WIV found most disturbing. From establishing which arguments were used, we can then move on to finding out how these arguments were brought forward: using tactics of resistance, or not?

The aim of the discourse analysis of the debate around the WIV is to find out how the opposers of this law resisted the securitizing language of the government and other actors in favour of the WIV. As mentioned in the theoretical framework, resistance against a securitizing move can come in three forms: desecuritization, counter-securitization, and delegitimization.

To categorize desecuritizing language, the framework of Hansen (2012) will be used. While two of the ways in which desecuritization occurs are passive, the other two, being replacement and rearticulation, can potentially be spotted as strategies used by opposers of the WIV. Discourse of replacement is when actors try to move the attention from the problem of terrorism to another, supposedly bigger problem. When this happens in an article, it can be pointed out quite easily. Rearticulation can be spotted if the speech act contains a solution to the problem of terrorism that is different from the security measures being proposed now (i.e. the WIV).

Next is counter-securitization. To judge whether counter-securitizing language is being used by a certain actor, we will look at whether the speech act follows the grammar of security: the securitizing language should contain a claim, a warning, a demand and supporting evidence of the claims. Furthermore, the message should contain a threat that is concrete and recognizable to the public. This last criterium might be difficult to assess, but we can assume that terms like ‘privacy violation’ or ‘human rights violation’ are concrete enough.

Lastly, delegitimizing discourse can be identified through the principles of legitimacy as illustrated by Balzacq (2019). Speech acts opposing the WIV could either critique the legality of the WIV, by saying it is illegal. Furthermore, they could target the justifications given by the state. According to Balzacq’s framework, this means that the law would not contribute to

the common values of society. Arguments made about the (dis-)proportionality or the (un-)necessity of the WIV will also be interpreted as de-justifying and thus delegitimizing arguments.

It is also important to keep in mind the views the public, both in general and, whenever possible, also the views of groups of people that can be (roughly) seen as the audience of a certain medium or political party. Researches including opinion polls and surveys have been consulted for the context chapter, and this information will be used to interpret the results of the research.

## Analysis

In this chapter, the results of the discourse analysis will be presented. This will be done in three steps. First, an overview of the main arguments given by opposers of the WIV will be given. Second, the findings relating to the use of resistance tactics are described. These results will be discussed in three subsections, one of them dealing with discourse by political parties and politicians, one of them dealing with NGO's and interest groups, and one of them dealing with opinion makers making an appearance in newspapers, tv shows or online. Last, an overview of the discourse will be presented, identifying relationships between the usage of a certain discourse and the role, political positions and audiences of actors.

## Arguments

While analysing the material that was found on the WIV-referendum, quite a large range of different arguments could be identified. This chapter will go through all of the arguments and describe how the arguments were presented. Unlike the analysis of the resistance tactics sequencing this chapter, a division will not be made between the various types of actors. The first arguments that are presented, about the WIV violation privacy, the sharing of data with foreign services, insufficient checks on the services and about the efficacy of the WIV, are the arguments that were used the most by opposers of the WIV. These arguments are followed by other arguments, that were used less frequently.

*The WIV infringes on privacy and civil liberties*

This is the argument that the initiators of the referendum, and many of their supporters, base their opinion on. Many of the other arguments that are used in the opposers' discourse relate to, or are based on this point. One of the students explains in tv-show Radar (25 Sep 2017):

"This is important to everyone because it is not only about the pictures of cats you look up on the internet. It is about your medical data, your locations, your search history. *Your privacy is fundamental to many other rights.* To freedom of press, to medical protection. And that is why it is important to every Dutchman"[3]

[3] Dit gaat iedereen aan omdat het niet alleen gaat om de kattenplaatjes die je bekijkt op het internet. Het gaat ook om je medische gegevens, je locaties, je zoekopdrachten. Je privacy staat fundamenteel aan een heleboel rechten. Aan de persvrijheid, aan medische bescherming. En daarom gaat het iedere Nederlander aan.

This view is shared by the majority of other actors. Articles that, for example, deal mainly with the freedom of press (Transparency International, 10 Oct 2017), the chilling effect (Privacy Barometer, 12 July 2017), or the sharing of information often also refer to the more general argument of privacy violations. The privacy argument can thus be seen as a connecting concept between all the other arguments.

*Sharing with foreign secret services*

According to the WIV, the Dutch intelligence agencies are allowed to share the bulk-data they collect with foreign intelligence services without checking the contents of such datasets. According to opposers of the law, this means that data on Dutch citizens could fall into the hands of other states, that might not respect human rights and data protection laws to the same extent as the Dutch government does.

This argument is brought forward by almost all actors opposing the WIV, and thus it appears to be one of the most important reasons for people to be against this law. The argument is, unlike for example the protection of journalists, brought forward by actors throughout the whole political spectrum. The majority of actors seems to have trust in the Dutch government and its intelligence services, and does not directly expect our own agencies to abuse the information collected with the WIV. However, they seem all the more worried about what foreign services can do with this information.

"The biggest danger for civilians does not come from the AIVD or the MIVD, but from foreign services, with whom we will be sharing massive amounts of our own data. This is information what we have not even been able to analyse ourselves, and of which we have no idea what it contains."[4] (SP, Feb 2018)

*The supervision on the services is not sufficient*

Many opposers of the WIV think that the law does not offer a sufficient guarantee of control by supervisory bodies (the TIB, who should grant permission for the use of mass digital surveillance in advance, and the CTIVD, who should check whether the permission was granted rightfully) over the security agencies. This is an argument that is mentioned by almost all actors opposing the WIV, though the emphasis that is put on this particular argument differs greatly per actor. The argument is quite complex and legal and not very 'sexy', but still

[4] Maar het allergrootste gevaar dat burgers lopen komt niet van de AIVD of de MIVD, maar van het optreden van buitenlandse diensten. Met wie wij massaal gegevens gaan delen van onze eigen mensen, informatie die wij niet eens hebben kunnen analyseren en waarvan we helemaal niet weten wat erin staat.

it is one of the most important deficits that opposers of the law want to point out. Of all political parties that spoke out against the WIV, only the PvdD and the Piratenpartij mentioned the problem with supervision. The PvdD, as the only party doing so, spent a relatively large portion of their article on this issue and the Piratenpartij elaborated on it in a long Q&A article which contained more technical aspects of the law.

NGO's and experts, writing in opinion magazines or newspapers, or appearing in tv-shows, spent a far larger part of their attention on the supervision problem.

Bits of Freedom (date unknown) writes that "the supervisory body should be able to show its teeth, if the services are acting against the law, the CTIVD should be able to stop them directly. The law should be amended so that the judgements of the supervisor are binding.[5] Nieuwsuur (10 Oct 2017) quotes the Raad van State (advisory institution of the government), saying that the TIB "would become a stamping machine, having an 'alibi function'."[6]

*The "dragnet" is not effective*

With all arguments presented it could be seen that they were somewhat related to each other, as they could all be linked to the argument of privacy violations and civil liberties. Therefore, in most publications that were analysed, a combination of several arguments was often presented. An exception to this rule is the argument of efficacy, which is not so much connected to privacy. Nieuwesteeg (Financieel Dagblad, 15 March 2018) makes an interesting point, saying that opposers should not so much refer to privacy arguments, since (following the theory of securitization) such arguments will most likely be beaten by arguments on security. Therefore he suggests to focus solely on the efficacy of the law, leaving behind all arguments on privacy. However, this does not mean that efficacy-related arguments are not being provided in combination with privacy-related arguments: many actors combine the two types of arguments in their articles on the WIV, like the Piratenpartij (16 Mar 2018):

"It is a false contradiction to state that you should sacrifice your privacy, your freedom, for security. It has not been proven that security will indeed be increased with the new possibilities for the secret services. Until now, with every attack, it has turned out that the terrorists were already in sight. According to the Piratenpartij, we are not going to find the

[5] De toezichthouder moet meer tanden krijgen, als de diensten in overtreding zijn moet dit direct door de CTIVD gestopt kunnen worden. De wet moet worden aangepast zodat de oordelen van de toezichthouder bindend zijn.

[6] Er is veel kritiek op de commissie die te toestemming moet geven. Het zou een stempelmachine worden. De Raad van State heeft het zelfs over een alibi-functie.

needle in the haystack by making this haystack even larger. With well-targeted detection the services can make better use of their resources."[7]

*Chilling effect*

The chilling effect entails that internet-users (in other words, everyone) will be more cautious when searching for certain "sensitive" topics online. This argument was not mentioned very frequently when looking at the whole sample, but it did form an important part of the rhetoric of the NGO and interest group actors. The chilling effect is not an argument that everyone knows of or understands, and therefore, in many cases, actors explained what it entailed and provided some scientific evidence to support this claim. In general the NGO and interest group articles were very informative, and the arguments used by these actors were, in general, well explained. Sometimes, other media take over the explanations of the concept from such organizations, as GeenStijl (21 September 2017) did with an article published by the Privacy Barometer (12 July 2017):

"The law has an intimidating effect. Large-scale surveillance will make people more careful. You never know whether the authorities are monitoring what you are doing online. Research by the University of California shows that after the Snowden-revelations, pages with terrorism-related subjects were visited 20% less (…), according to the researcher, 'the fear for government surveillance leads to a form of self-censorship that we normally see in police states'."[8]

Other actors, such as political parties, sometimes referred to the chilling effect briefly, like GroenLinks who stated that "consciously or unconsciously, people will watch out for what they write".[9] Referring to the concept in this way, however, was seen less often.

*Protection of journalists and their sources, lawyers, and doctors and their patients*

The argument that the WIV lacks adequate guarantees to protect journalists and their sources is brought forward by Transparency International (10 Oct 2017) and Free Press Unlimited (12

[7] Het is een valse tegenstelling om te stellen dat je jouw privacy, jouw vrijheid moet opgeven voor veiligheid. Er is niet bewezen dat de veiligheid daadwerkelijk zal vergroten met de nieuwe mogelijkheden van de geheime diensten. Tot nu toe is bij iedere aanslag gebleken dat de daders reeds in beeld waren. Wat de Piratenpartij betreft gaan we de naald in de hooiberg niet vinden door deze hooiberg nog groter te maken. Met gerichte opsporing kun je je middelen veel beter inzetten.

[8] Er gaat een intimiderende werking van de wet uit. Grootschalig afluisteren van internet zal mensen voorzichtiger maken. U weet immers nooit of de autoriteiten meekijken bij wat u op internet doet. Een onderzoek van de universiteit van Californië laat zien dat na de Snowden-onthullingen, pagina's met terrorisme-gerelateerde onderwerpen 20% minder werden bezocht. Een ander onderzoek laat zien dat 34% van de mensen terughoudender op internet wordt door het grootschalig afluisteren. Volgens de onderzoekster "dwingt de angst voor overheidscontrole tot een vorm van zelfcensuur die we normaal in politiestaten zien.

[9] Bewust of onbewust zullen velen rekening houden met wat ze schrijven

Sep 2017) as the most important argument for opposing the WIV. This is logical, given that both organizations are involved in protecting the interests of journalists and whistle-blowers, who would be directly hurt by this deficit of the law. The argument was taken over by all political parties that spent a large amount attention to the topic (GreenLeft [GL], Socialist Party [SP], Party for the Animals [PvdD], Pirate's Party [PP]), as well as by some opinion makers, such as Maurits Martijn and Dimitri Tokmetzis at 5 Uur Live (RTL, 27 Feb 2018):

"The information of a journalist can end up in Zoetermeer (*AIVD Headquarters*). And the same goes for attorneys, who are afraid that the communication with their client, that is confidential, is also picked up by the dragnet. (…) And they are afraid that they cannot confidentially communicate with their clients anymore"[10]

*Future rulers / data getting into the wrong hands*

This argument entails that the possibilities this law gives the government might be abused by future rulers. It is similar to the previous argument in the sense that is does not deal with what our current government, in which the Dutch generally seem to trust, can do with the law, but what others can do with it. Arjen Lubach, in the episode of his tv-show in which he massively boosted the campaign to collect the necessary signatures to force a referendum, actually named this as the main reason for wanting this referendum:

Fragment Showing Interior Minister Ronald Plasterk: "Some people think that [the WIV] comes with the fact that we will be *en masse* looking into the (tele)correspondences of Dutch citizens, and that is certainly not our intention"

Lubach: "No, of course that is not your intention Ronald Plasterk, but I trust you (…). But it is not about Ronald Plasterk, because he will be gone in two weeks. But who comes after him? And after that? You can just never be sure what lunatic will get in charge [shows picture of Trump]. This dude just yesterday has requested data of everyone who has liked a certain anti-Trump Facebook page. So in America you should already seriously watch out which pages you visit. I mean, what if something happens here?"

Fragment of Plasterk: "That is certainly not our intention"

[10] Daarvan kan dan de informatie in Zoetermeer komen te liggen. – Geldt bijvoorbeeld ook voor advocaten, die zijn bang dat de communicatie die zij met hun client hebben, die vertrouwelijk is, en al heel vaak geschonden wordt overigens, dat die ook in dat sleepnet worden meegenomen. En die zijn bang dat die niet meer op een vertrouwelijke manier met hun cliënten kunnen communiceren.

Lubach: “No, that is not your intention, but it *could* happen. If some kind of idiot comes into power, then they could maximally stretch this law that is too vague.”[11]

*Retention term*

Data collected by the security services through the WIV can be retained for a period of three years. Various actors have argued that this period is too long. They mainly base this argument on the fact that these retention terms in other (European) countries are generally shorter. However, all actors that mentioned this argument did so only briefly, and this argument was not identified in any article to be a leading argument.

*Invalid accusations, discrimination and (ethnical) profiling*

Another argument that was not very prominently present throughout the whole sample of articles, but still it was mentioned a couple of times. Some actors seem to be worried that the WIV, and the big data-driven intelligence tactics that might come with them, will lead to an increase in ethnical profiling and discrimination, which will then lead to invalid accusations of, most likely Muslim or foreign, people. Most sources referring to this problem (Gijzen, 15 March 2018 and Rumulova, 15 March 2018) refer to the facts that algorithms might contain some bias towards people from minorities, or that algorithms can simply contain mistakes.

GeenStijl, quite remarkably, given it is a (far) right-wing weblog, goes one step further, suggesting the WIV “could lead to a general violation of the rights of all Muslims, also the innocent, hard-working believer who, in his own time, is ‘by coincidence’ a Muslim. The dragnet makes such ‘specification’ of demographic groups easier, with large potential consequences”[12]

[11] Fragment: Plasterk: “Sommige mensen denken dat dat met zich meebrengt dat we massaal in de correspondentie of telefonie van Nederlandse burgers zouden kunnen gaan rondneuzen, en dat is zeker de bedoeling niet.” Lubach: Ja nee natuurlijk is dat niet jouw bedoeling Ronald Plasterk, maar jou vertrouw ik. (...) Maar het gaat niet om Ronald Plasterk, want die is over twee weken weg. En wie komt daarna? En daarna? Je kunt gewoon nooit weten wat voor gek er aan de macht komt. (toont foto van Trump). Deze knakker heeft gisteren nog de gegevens opgevraagd van iedereen die een bepaalde anti-trump facebooksite heeft geliked. Dus in Amerika moet je nu al serieus oppassen waar je op klikt. Ik bedoel, wat als er hier zoiets gebeurt? Fragment: Plasterk: “nee dat is zeker de bedoeling niet.” Lubach: Nee dat is niet de bedoeling, maar het kán dus. Als hier echt een stelletje idioten aan de macht komt dan kunnen ze die veel te vage wet maximaal gaan oprekken.

[12] De kans die er nu is om gericht te zoeken naar subversieve predikers in haatzaaiende moskeeën (en die door het ‘speld in een stapel spelden’-effect van een Sleepwet wordt verspeeld) zou dan wel eens om kunnen slaan naar een algehele schending van de rechten van alle moslims, óók de brave, hardwerkende gelovige die in zijn eigen tijd ‘toevallig’ moslim is. De Sleepwet maakt zulke ‘specificatie’ van bevolkingsgroepen makkelijker - met alle potentiële gevolgen van dien.

*The WIV targets innocent citizens*

The fact that the WIV does not only target potential suspects of criminal or terrorist activities, but that it might influence innocent citizens as well, is something that is mentioned by the majority of sources. There is one notable difference between the usage of this argument and the usage of all the arguments mentioned before, and that is that this argument is mostly mentioned between the lines, and not as a main point. An example which illustrates this well comes from the article by the Socialist Party (SP) (Feb 2018), which states "It is questionable whether the mass collection of data of innocent citizens is necessary and effective to prevent terrorist attacks from happening."[13] This is mainly an argument on the effectiveness of the WIV, but the fact that innocent citizens are being targeted was also included. Throughout all sources, "innocent people" or "innocent citizens"[14] were mentioned over 57 times, making this an important argument in the debate.

## Resistance Tactics

The next section will analyse the resistance tactics used by all three types of actors opposing the WIV. This part of the analysis will be split out into three parts because by doing this it may be easier to create a good overview of the tactics used throughout the whole spectrum, and to find patterns within and across the three sections. The three categories of resisting discourse will be analysed separately, and within the sections on political parties and on opinion makers, actors will be organized according to their place in the political spectrum. While there is no way to measure exactly to what extent an actor is left-wing or right wing, it is clear of most actors whether they are generally perceived to be left-wing or right-wing, and this general perception can be used to organize the analysis. The first section of this chapter deals with political parties, followed by NGO's, and finally opinion makers.

## Political Parties

*Desecuritization*

While analysing the discourse used by political parties in the WIV-debate, desecuritizing discourse was not discovered. No political party stated that terrorism is not that much of a security threat, making privacy-violating intelligence laws unnecessary. It is possible that this

[13] Het is maar zeer de vraag of het massaal binnenhalen van gegevens van onschuldige burgers noodzakelijk en effectief is voor het voorkomen van aanslagen en het bestrijden van terrorisme
[14] Onschuldige mensen; onschuldige burgers

is the fact because there is a large consensus that terrorism is actually a security issue, so stating otherwise would not be very effective. Most parties actually acknowledge that terrorism is a security issue, and that it should be fought. They just think this should be done using other methods: "Preventing attacks is done by accurately following terrorists and radicalized Salafist networks, the collecting of data of innocent citizens using a 'dragnet' will not help with that."[15] (Van Raak, Feb 2018)

*Counter-securitization*

Contrary to desecuritization, the strategy of counter-securitization is visible in almost all the sources that were published by political parties. There is difference, though, in the extent to which securitization is used as a strategy, and in whether the grammar of security can be identified throughout the articles.

On the left side of the political spectrum, the SP and the PvdD went the furthest with securitizing discourse. The Socialists, in their longer article on their web site (Feb 2018), set the tone already in the title, writing (all in caps): "THE DRAGNET IS UNNECESSARY AND DANGEROUS".[16] Opening the article like this, the party directly makes clear to its audience that it perceives the new law to be dangerous. After this opening, the article continues by providing the reader with arguments on the necessity and the efficacy of the law, before continuing the discourse on the potential dangers on the law. This part of the article is illustrated by an image from a film and the sentence: "Will the government be watching us from our attics, like in the film The Life of Others?"[17] Since this image and this sentence sketch a very dystopian future, this can be interpreted as securitizing discourse. Furthermore, the article suggests that the WIV is dangerous because it allows our secret services to share the data of citizens with foreign services. The sentence "But the utmost danger does not come from the AIVD or the MIVD, but form the acting of foreign services"[18] clearly contains a message of danger.

The grammar of security, consisting of a claim, a warning, a demand and supporting evidence of the claim, is present in this article. The claim is mainly that the dragnet is unnecessary and dangerous, the warning is an increase of government surveillance and the threat from foreign

[15] Aanslagen voorkomen doe je door gericht terroristen te volgen en geradicaliseerde salafistische netwerken te ontmantelen, het met een 'sleepnet' massaal binnenhalen van gegevens van onschuldige burgers helpt daarbij niet.
[16] DE SLEEPWET IS ONNODIG EN GEVAARLIJK
[17] Zit de overheid straks bij ons op zolder, zoals in de film Das Leben der Anderen?
[18] Maar het allergrootste gevaar dat burgers lopen komt niet van de AIVD of de MIVD, maar van het optreden van buitenlandse diensten.

services, the demand is the suspension of the WIV, and the arguments mentioned throughout the articles provide evidence supporting the claims.

The PvdD tries to get the urgency of the matter across by securitizing the concept of privacy. At two points in the article (date unknown), the connection between privacy and security is directly made: "Privacy offers us security and protects us from the state. When we give up our privacy, we give up an important part of our security"[19] and "The Party for the Animals thinks privacy is security".[20] By implying privacy and security are closely related, and by stating that the WIV infringes the right to privacy of citizens, the WIV is thus framed as a threat to the security of citizens. Just like in the SP article, supporting arguments to this claim are provided, and a call to action is made: vote against the WIV to stop the government from violating our privacy, meaning the grammar of security is also followed in this article.

Next to this article, the PvdD also published a short video, in which the same rhetoric is used. In the video, 'security' is represented by a dinosaur, that ends up eating the person it is supposed to protect, implying that too much security might end up being a danger itself. Furthermore, the final words of the video, "feel free to vote no, against the dragnet, for all security" show a clear call to action, plus they imply that by voting against the WIV, people will increase their own security.

Moving a little to the centre, though still on the left, is GL. This party has clearly chosen to present the voter with a much more moderate story. Though the party is a fierce opposer of the WIV, it has not chosen to use the grammar of security to convince its voters to vote against the new law. Instead, a wide range of arguments is presented. One time it is mentioned that the law could potentially have dangerous implications, because the fact that the dragnet tactic might not be effective might have as a consequence that terrorists will have an increased chance of success ("bulk data kills people"), but this is not a main theme of the article, and it is not aimed at the securitization of privacy violations as a whole.

Moving to the far right side of the political spectrum, we find FvD. While SP, PvdD and GL all wrote rather long articles on the topic, FvD only made a video (10 Mar 2018), that was published during the phase in which the signatures for the referendum were still being collected. In the video, FvD does not chose to follow the grammar of security. It does, however, refer to Orwell's 1984 with the sentence "Big Brother will be watching you!". This

[19] Privacy biedt ons veiligheid en beschermt ons tegen de staat. Wanneer we onze privacy opgeven, geven we een belangrijk deel van onze veiligheid op
[20] De Partij voor de Dieren is van mening dat privacy veiligheid ís

reference to a dystopian future, in combination with the ominous music playing in the background, could be interpreted as a 'flirt' with securitization, but as the grammar is not present, it will not be considered a proper securitizing move.

Last is the Pirate's Party, a one-issue party occupied with defending online freedom, and therefore an interesting player in this debate. In its campaign video (30 Jan 2018), the party states "a dangerous law is coming, a threat to our civil rights and the way in which we handle communication"[21], a sentence which implies there is a link between the WIV and security. Furthermore, someone in the video says "in some countries the population is being monitored 24/7"[22], a similar dystopian discourse that was seen in other articles, referring to e.g. 1984. By calling the WIV "a dangerous law", "a threat to our civil rights", and "fucking bad", providing supporting arguments to these claims, and by calling upon its public for action, the grammar of security was followed during the video.

Next to this video, the Pirate's Party also published a longer article (16 Mar 2018) on its web site, on which it provides the reader with answers to questions they might have on the WIV and the referendum. In this article, the discourse is a lot more nuanced. No securitising rhetoric is used, and the party tries to give correct and often rather technical answers to the questions.

*Delegitimization*

Unlike counter-securitizing discourse, delegitimization is not visible in the majority of publications by political parties. Furthermore, in the articles that the strategy is visible in, it is less prominently present.

As mentioned above, SP opens its article with "The dragnet is unnecessary and dangerous". Next to the securitizing message that this sentence contains, there is also a delegitimizing message in the word "unnecessary".[23] Furthermore, SP takes over the term invented by Arjen Lubach, 'terreurschwalbe' ('terror-dive')[24], to point out that the arguments provided by proponents of the WIV, namely that the law is necessary to prevent terrorist attacks from happening, are untrue. By treating the proponent's arguments as such, it can be argued that SP

[21] Er is een gevaarlijke wet op komst. Een bedreiging voor onze burgerrechten en de manier waarop we omgaan met communicatie.
[22] In sommige landen wordt de bevolking 24/7 digitaal gecontroleerd
[23] Onnodig
[24] Schwalbe is a German/Dutch football term for a fake dive

is trying to draw doubt to the legitimacy of the actors using these arguments. In total, the unnecessity of the WIV is mentioned three times in the article.

PvdD also writes that the WIV is unnecessary. In the opening paragraph of the article, the sentence "unnecessary, because from research on terrorists it appears they were already in view of the secret services".[25] Furthermore, the party writes that it "will never tolerate that our human rights, our civil rights, will be risked for false security"[26], thereby implying that the law will not provide any security at all. As this means that the law, not contributing to security and not contributing to civil rights, would not contribute to the common values of society and thus not justified.

The Pirate's Party does not speak in terms of 'terreurschwalbes' or 'false security', but does provide a delegitimizing argument for the tech-savvy reader, as it also deems the dragnet unnecessary. In its FAQ article, the party explains a dragnet would not be necessary and that the same amount of data on suspicious persons can be collected without collecting the data from the whole neighbourhood.

**NGO's and interest groups**

*Desecuritization*

Similar to what we saw in the political discourse, desecuritizing language was not used by NGOs and interest groups. Instead, worries about the secret services not being able to fight terrorism with the new WIV were shared, proving terrorism is seen as a serious threats by those NGO's fighting the new law as well.

*Counter-securitization*

Most NGO actors did not make use of securitizing discourse to get their point across. No cases of a true securitizing move, following the grammar of security, were found. However, this does not mean that there were no cases at all in which potential dangers of the WIV were considered.

Two organizations, being Bits of Freedom (date unknown) and Privacy First (13 Mar 2018) shared their concerns about the fact that secret services are allowed to hack other institutions,

[25] Onnodig, want uit onderzoek naar aanslagplegers bleek dat zij allang in beeld waren bij de geheime diensten
[26] Wij zullen nooit tolereren dat onze mensenrechten, onze grondrechten op het spel worden gezet voor schijnveiligheid.

and that they do not have to report the weak sport they used to do so to the network owners. Privacy First writes that "because of this, potential malicious actors can abuse these weaknesses."[27] Bits of Freedom adds to this "by not notifying the makers of these weak spots, the secret services do not makes use safer, but more unsafe."[28] Notable is here of course that the organization chooses to use the word 'dangerous' in this sentence, creating urgency for this problem.

Another noteworthy sentence used by Privacy First, when writing on problems the WIV could bring to the protection of journalistic sources, is "and when we lack proper news coverage, the democracy malfunctions".[29] More than a threat to privacy, a threat to democracy implies a danger to our society, meaning this phrase could be interpreting as having a securitizing intention. The grammar of security, however, was not followed, making it no more than a 'flirt' with securitization.

*Delegitimization*

Just like securitization, delegitimizing strategies were also used by two organizations, the most prominent of which is Amnesty International. Amnesty is an interesting actor in this debate, having played an important role in the start-up phase of the referendum because it was one of the first and largest organizations that picked up the idea to initiate a referendum. First, Amnesty calls into question the necessity of the law by writing "[the WIV] unnecessarily threatens our privacy and our freedom of expression".[30]

After this, Amnesty writes the following: "The commitment of the government that 'of the random and massive collecting data of citizens in the Netherlands and abroad can, will and shall be no question' is meaningless. In a state with the rule of law, legitimate acting of the government is never random. The government does not write random tickets, and does not collect random taxes. And the massive collection of data is exactly was is aimed for with the dragnet."[31]

[27] Hierdoor kunnen eventuele kwaadwillenden (langdurig) misbruik maken van deze kwetsbaarheden.
[28] Door deze zwakke plekken niet te melden bij de maker, maken de geheime diensten ons niet veiliger maar juist onveiliger
[29] En als een goede nieuwsvoorziening ontbreekt, hapert de democratie.
[30] Omdat die onnodig onze privacy en vrije meningsuiting bedreigt
[31] De toezegging van de minister in het regeerakkoord dat 'van het willekeurig en massaal verzamelen van gegevens van burgers in Nederland en het buitenland geen sprake kan, mag en zal zijn' is betekenisloos. In een rechtstaat is legitiem overheidsoptreden immers nooit willekeurig. De overheid schrijft geen willekeurige boetes uit en legt geen willekeurige belastingen op. En het massaal verzamelen van gegevens is juist wat beoogd wordt met de sleepnetbevoegdheid.

With this statement, Amnesty does not just draw the legitimacy of the WIV into question, but even the legitimacy of the government as a whole, if it would implement this law. The writers made the aim of this passage very clear by making use of the word 'legitimate'.

Privacy first tries to delegitimize the government by stating it spreads fake news to convince the people to vote in favour of the WIV: "Fake news by the Dutch government: according to our interior minister Ollongren it is not necessary that the government places neutral information about the dragnet-referendum on het web site government.nl. Because of this, the government does not spread objective information to the electorate."[32] The most nuanced interpretation of this text would be that the government does not do enough to inform the people about the referendum. The words 'fake news', however, could also be interpreted as if they imply that the government is providing the people with incorrect information or lies. Making such a statement can be interpreted as delegitimizing as it draws the good intentions of the government into question.

Important to note is that both 'drawing the integrity of a government into question' and directly 'drawing the legitimacy of a state or government into question' were not described in the theoretical framework as indicators of delegitimizing discourse. However, it would be safe to say here that the intention of the writers of these texts was to do so, and therefore they were named here as examples of delegitimizing discourse.

## Opinion Makers

### *Desecuritization*

Opinion makers also did not make use of any desecuritizing discourse and also all seem to agree on the fact that terrorism indeed forms a security threat. The example that best shows this of all articles is the part on the "WIV-Belsivboom" ("WIV-decision tree") by Arjen Lubach (18 Mar 2018), in which he says "Everyone wants to prevent attacks! Except those few that commit them."

### *Counter-securitization*

In the landscape of opinion makers, counter-securitizing discourse was visible in various sources. However, there were big differences between the sources in the amount of

[32] Fake news door Nederlandse overheid
Volgens onze minister van Binnenlandse Zaken Ollongren is het niet noodzakelijk dat de overheid op haar website rijksoverheid.nl neutrale informatie plaatst over het Sleepwet-referendum. Hierdoor wordt er door de overheid geen objectieve informatie verstrekt aan de kiezers.

securitizing discourse that was being used. One section of the opinion landscape in which this kind of language was relatively prominent is the weblogs. Both on the left side of the political spectrum (Joop!) and on the rights side (GeenStijl), the strategy of securitization was used.

The analysis once again starts at the left side of the spectrum. On the weblog Joop!, Jelle de Graaf (7 Oct 2017), who was a prominent member of the Pirate's Party at that time[33], writes "the democracy is under fire"[34], "this referendum gives us a second chance to avert this threat to our democracy"[35], and "the saving of those data for three years, an extreme term compared to other countries, is an unnecessary danger"[36]. By using this language, the author issues a warning, and provides a call to action, most clearly in the title: "save the democracy, stop the dragnet"[37]. Also, the writer provides supporting arguments in his article, thereby following the grammar of security.

Another author publishing on Joop!, Han van der Horst (14 Mar 2018) spreads a generally less securitizing message. However, the writes does not refrain from referring to the Nazi occupation of the Netherlands, a similar move to the references made to the GDR by other authors.

On the other side of the spectrum, GeenStijl (14 Mar 2018) did not refrain from using securitizing language when writing on the referendum. It is generally known of this weblog that they never refrain from using strong, unnuanced language, and it could be seen as part of their trade mark. The first article on the WIV opens with "It is bizarre that a dragnet could be designed, it is frightening that a political majority wanted to approve it and it is mortifying that millions of citizens don't give a fuck"[38], a text that is complemented with a drawing of interior minister Ollongren pictured as Medusa, with cameras in her hair. Later in the article, the government is portrayed as a "jealous Stasi" and it is written that it can't be guaranteed that the government will be spying on its citizens. By terms as 'frightening' and 'mortifying', a sense of threat is suggested, though the words are not exactly aimed at the WIV itself, but on the fact that the people seem to accept this law without any problems. The title of the

[33] This article was written on his personal title
[34] De democratie ligt onder vuur
[35] Dit referendum geeft ons een tweede kans deze bedreiging voor de democratie af te wenden
[36] Het opslaan van die gegevens voor drie jaar lang, een extreme tijd in vergelijking met andere landen, is een onnodig gevaar
[37] Red de democratie, stop de sleepwet!
[38] Het is bizar dat een Sleepwet kon worden ontworpen, het is beangstigend dat een politieke meerderheid hem wilde aannemen en het is dood- en doodeng dat het miljoenen burgers geen fuck boeit dat het gebeurt.

article, “the Dutch are dragnet-sheep”[39], is another reference to this. Also, the Stasi-reference is a flirt with securitization.

In another article (21 Sep 2017), GeenStijl makes a similar point by comparing the current Dutch situation to Turkey, in which a democratically elected leader abuses the powers of security agencies to reinforce their own position. Both articles make clear that GeenStijl sees danger in the WIV. However, the grammar of security is not followed in both articles.

Moving on to media that are a little more established, or ‘mainstream media’, and starting again on the left of the spectrum, we arrive at De Correspondent. In an article in this online news magazine, the chief editor (Wijnberg, 20 Mar 2018) writes “Myself, I belong to the school that states we should not create the illusion that risks such as terrorism are puzzles. Because that opens the door to a totalitarian state, that wants to know everything of everyone. Then, there is no argument left not to turn the ‘dragnet’ in the WIV 2017 into an ever-present Big Brother. You do not want to have future blood on your hands, do you?”[40] In this discourse, Wijnberg refers to the potential dangers of a surveillance state, and the WIV could be the next step in this direction if the people don’t take action. The last part of the sentence includes a message of action, since it suggests that if the reader does nothing (i.e. does not vote against the WIV), they could potentially have blood on their hands. Furthermore, Wijnberg writes he prefers to live in a time in which “we understand that security has as its goal to protect those fundamental rights, privacy and freedom”[41], connecting privacy and security with each other.

On the other side of the ‘main stream’ section, in the Telegraaf, writer Leon de Winter (20 Mar 2018) published an opinion article called “In a while, Orwell’s 1984 will be a fact”, another article that sketches a situation in which the WIV is a prelude to a dystopian future. Also, by naming the government “the most powerful, and thus sometimes the most dangerous party in society”[42], the connection to danger has been made. In the same edition of this newspaper, Rob Hoogland (20 Mar 2018) wrote a very similar article. It is called “Big Brother” and makes a connection between the WIV and the securitiy apparatus in China:

[39] Nederlanders zijn sleepnetschapen
[40] Zelf behoor ik tot de school die stelt dat we niet de illusie moeten kweken dat risico’s zoals terrorisme puzzels zijn. Want dat opent de deur naar een totalitaire staat, die alles wil weten van iedereen. Er is dan geen enkel argument meer voorhanden om van het ‘sleepnet’ in de Wiv 2017 niet uiteindelijk een alomtegenwoordige Big Brother te maken. Je wilt toch geen toekomstig bloed aan je handen hebben?
[41] een tijd waarin we begrijpen dat veiligheid uiteindelijk als doel heeft juist die grondrechten, privacy en vrijheid, te waarborgen?
[42] En het is de machtigste, en dus soms gevaarlijkste, partij die de samenleving kent.

"Let's for now, when I comment on the law on which we can have our say tomorrow, not refer to Orwell's 1984. In Beijing Big Brother is watching much more emphatically. In China you are – completely screwed"[43]

In other mainstream media, there are not so many examples of securitizing discourse to find. In NCR, Marc Hijink (20 Mar 2018) briefly mentions the fact the hacking methods of secret services frequently leak, something which poses a "danger to everyone"[44]. Axel Arnbak, a lawyer who debates the WIV in the tv-show Buitenhof (4 Mar 2018) once describes the WIV as "a nuclear option, if you put this into law, it is a little like the spectre of a Big Brother that will tap everything", which in itself can be seen as securitizing language, but since it is only one sentence in a 17-minute debate it was certainly not the main discourse. Furthermore, there are many other sources published by mainstream media, both on TV and in paper, that did not use any securitizing language while arguing against the WIV.

The last actor that will be analysed is the group of students that initiated the referendum. On behalf of this group, Marlou Gijzen was interviewed by Algemeen Dagblad (Rosman, 17 Mar 2018), and wrote an opinion article in De Volkskrant (15 Mar 2018). In AD, Gijzen is quoted saying "privacy is essential for security"[45] , connecting the two concepts. In De Volkskrant she writes that the right to being innocent until the opposite has been proved is being undermined by the WIV, and asks "isn't this right fundamental to democracy and the rule of law?"[46], implying the WIV forms a threat to this rule of law. Furthermore, in an item on TV show EenVandaag (21 Mar 2018), on of the initiators securitizes privacy by saying "It is not for nothing that privacy is a human right, it is there to keep you safe against the government, and when that right gets violated, we actually all are more unsafe."[47]

*Delegitimization*

Similar to what we saw in the political discourse, the strategy of delegitimization was used less frequently than securitization by opinion makers, but still there are plenty of examples of such discourse to be found. In Joop!, Jelle de Graaf (7 Oct 2017) calls the "large-scale,

[43] Laat ik voorlopig, als ik de wet waarover wij morgen iets mogen zeggen wil becommentariëren, dus maar niet naar Orwell's 1984 verwijzen.
In Peking kijkt Big Brother al veel nadrukkelijker toe.
In China ben je
helemáál de sjaak
[44] Dat is een bedreiging voor iedereen
[45] Veiligheid begint juist met privacy
[46] Is dit recht niet van fundamenteel belang voor onze democratische rechtsstaat?
[47] "Het is niet voor niets dat privacy een mensenrecht is, dat is er om jou juist veilig te houden tegen de overheid, en zodra dat recht wordt geschonden zijn wij eigenlijk allemaal onveiliger."

random collection of internet traffic of people that are not suspected of anything is a grave and disproportionate privacy breach"[48], and later in the article he makes makes a similar comment: "[the WIV is] an unnecessarily large, long-term and disproportionate privacy violation"[49]. By targeting both the proportionality and the necessity of the law, the writer questions the legitimacy of the law.

GeenStijl (14 Mar 2018) questions the necessity of the law by saying the secret services should focus their attention to people that "undermine the democracy, preach hate and/or spill blood (…) and that can be done without a dragnet for all citizens".[50] Furthermore, GeenStijl argues that the law is not effective, and even illegal, hereby definitely saying the Wiv cannot be legitimate: "the new dragnet-law gives secret services far-going instruments that are not effective in the fight against terrorism. Instead, these instruments are intimidating and even unlawful."[51]

Other media that write on the necessity and proportionality are the Volkskrant (29 Jan 2018), that writes "expansion of the tapping authorizations is unnecessary"[52] and the Groene Amsterdammer (15 Mar 2018), writing "the *Raad van State* also wondered in a reaction on the new intelligence law whether large-scale data collection meets the proportionality requirements of the European Treaty of Human Rights"[53]. Experts discussing the WIV in the TV-show Radar and Nieuwsuur also ask the question whether the WIV is proportional, without giving an answer to this question.

Lastly, part of the item made by Arjen Lubach can be seen as delegitimizing. However, Lubach does not target the law itself in this part, but the people that argue in favour of this law. He describes the 'terreurschwalbe' or 'terror-dive', with which he suggests the government and other proponents of the WIV use false arguments to convince people of the necessity of this law. He continues this point later in the item by saying "Ollongren says the services are not allowed to tap the cable. That sounds very inconvenient, but it is not right.

[48] Het grootschalig, ongericht verzamelen van internetverkeer van mensen die nergens van verdacht worden is een grove en disproportionele inbreuk op de privacy.
[49] Een onnodig grote, langdurige en disproportionele inbreuk op de privacy
[50] De democratie ondermijnen, haat zaaien en/of bloed vergieten (…) Dat kan prima zonder sleepwet voor alle burgers.
[51] De nieuwe sleepwet geeft geheime diensten verregaande bevoegdheden die niet effectief zijn in de strijd tegen terrorisme. Wel zijn de bevoegdheden intimiderend en zelfs onrechtmatig.
[52] Uitbreiding van aftapbevoegdheden is onnodig
[53] Ook de Raad van State vroeg zich in een reactie op de nieuwe inlichtingenwet af of de grootschalige gegevensverzameling wel voldoet aan de proportionaliteitseis van het Europees Verdrag voor de Rechten van de Mens

They are allowed to. (…) Prime minister Rutte last Friday came with the same delusion. (…) The problem is that it is not true. That the cabinet chooses to campaign by lying."[54]

## Discussion

### *Interpretation of findings*

When looking at the results of the discourse analysis, and keeping in mind the information from the theoretical framework and the fact and figures presented in the context chapter, a few interesting things can be noted. This part will go through these findings in the same order as was used in the analysis chapter. To start off, we take another look at the arguments used by the actors opposing the WIV.

### *Arguments*

The four arguments that were used the most by actors opposing the WIV were the following: (1) the WIV is infringing on privacy and civil liberties, (2) the WIV allows the services to share data with foreign services, (3) the supervision on the services is insufficient, and (4) the WIV is not effective to fight terrorism. These arguments to a large extent overlap with the arguments provided with people who voted against the WIV: (1) Privacy, (2) the WIV is not good in its current form (possible because of the sharing of data with foreign services, or because of insufficient supervision), (3) a lack of trust in politics, and (4) too few safeguards Jacobs et al. 2018). Only argument 3 cannot be traced back to the arguments provided by the opposers of the WIV in the media. As the main argument for those in favour was security, it is confirmed that securitization played a big role in the debate around the WIV.

A large part of the people that voted against the WIV can be found in the groups of young and/or left-wing voters. When we look at the sources that argued against the new law, it is visible that often they are also coming from the left corner (GL, SP, PvdD), or from media that are read/viewed by a largely young public (VICE, GeenStijl, Lubach). Another notable fact from the context part is that three quarters of the SP and GL voters voted against the WIV, while these were also the two biggest parties that campaigned against the law.

Taking all these factors together, there is a significant similarity between the actors campaigning against the WIV, and their arguments, and the people who voted against the

[54] Ollongren zegt dat de diensten niet mogen aftappen via de kabel. Dat klinkt inderdaad erg onhandig, maar het klopt niet. Dat mag namelijk wel. Premier Rutte kwam vrijdag namelijk met precies dezelfde misleiding. (...) Het probleem is dat het niet waar is. Dat het kabinet ervoor kiest om campagne te voeren door te liegen.

WIV, and their reasons to do so. It should therefore be safe to conclude that the actors campaigning against the new law managed to reach, and influence, their audiences.

*Desecuritization*

Moving on to the resistance tactics, the first is desecuritization. As was already clear during the analysis part, desecuritizing tactics were not used by any actor arguing against the WIV. Terrorism is a highly securitized subject, meaning it is seen as a security threat by (almost) every member of the public. A strategy that states terrorism is 'not too bad of a threat' almost certainly would not work, and would probably bring a lot of damage to a political actor in the case an attack would probably happen. Furthermore, as shown by examples in the analysis part, actors actually acknowledge that terrorism is a threat. Some actors subsequently made the choice to project the WIV as a larger threat than the threat of terrorism, bringing us to the next resistance tactic.

*Counter-securitization*

When looking at the usage of counter-securitizing language, it can be noted that it appears mostly with actors that are located on the flanks of the political spectrum, either the left or the right. SP and PvdD, being on the far side of the (parliamentary) political spectrum, have used the tactics the most of all parties that campaigned against the WIV. Moving to the centre-left, GL used the tactic a lot less, perhaps choosing to use some more nuanced language. Finally, at the far right side of the spectrum, FvD, to some extent, also used securitizing language. Similarly, media like Joop! and VICE, that are perceived to be very left-wing made use of securitizing discourse, just like GeenStijl, a medium located at the right flank. Notable exception to this rule is De Telegraaf, which can be seen as a slightly populist newspaper, but which cannot be described as far right (NOS Nieuws, 2 Jan 2018). NGO's and more centrist media, such as the NPO (public broadcasters) and some newspapers (AD, NRC, Volkskrant) did not or only sporadically use securitizing language.

What a large part of the actors using securitizing discourse also have in common is that they are generally known for using language that can be described as outspoken, unnuanced, or populist. De Telegraaf is well known for its bold headlines, GeenStijl for its provocative and sometimes even insulting style, and SP is often referred to as left-wing-populist. Keeping this in mind, it should not be surprising that it is exactly there actors that come forward as those that make use of securitizing discourse the most. The other way around, actors such as GL or

De Volkskrant, that do not have such a reputation, refrained from using such language. Whether an actor choses to frame the WIV as a threat to our security, or just as a threat to our privacy, could thus for a part be a stylistical choice.

There is a difference between the audiences of different political parties, media, NGO's, et cetera. It is logical that an actor aligns its message with the audience it wants to reach, and therefore different strategies will be used by different actors to get their point across. The theory on (counter-) securitization, however, does not explain whether there are certain groups that are more susceptible to securitizing language than others, so we do not know to what extent the fact that different actors have different audiences matters for their use of resistance strategies.

*Delegitimization*

Moving on to the final resistance tactic, in total, delegitimization language appeared less often in the sources that were analysed. However, the actors that did make use of these strategies do appear to be more spread out across the political and media spectrum. Furthermore, the strategy was also used by some NGO's. The question is why this is the case. The fact that more actors made use of the strategy might mean that delegitimization is a strategy that actors are more likely to resort to first, as if it is a less far-going strategy; claiming something is dangerous or a threat to our society might be seen as less of a bold statement as claiming something is unnecessary or disproportionate. The fact that a broader range of actors made use of delegitimizing language might mean a broader audience might be susceptible to such arguments.

In the theoretical framework, delegitimizing discourse was defined as such that it could appear in the following forms: (1) discourse stating the WIV is illegal, (2) discourse stating the government could not justify the WIV, (3) arguments stating the WIV would be disproportionate or unnecessary. These forms of delegitimization are mainly aimed at the security measure itself, and not at the actor imposing this measure. Such arguments, as mentioned above, were used throughout the spectrum by several actors, and there does not seem to be a specific target audience for it, neither does delegitimization seem to be the main strategy of the actors using it in this form. However, another form of delegitimization, that was not described as such in the theoretical framework, was discovered during the analysis.

Some actors accused the government, or other proponents of the new intelligence law, of misleading the voter, or, in other words, lying. The most important example of this is Zondag

met Lubach's 'terreurschwalbe' ('terror-dive'), with which is implied that the government uses the prospect of potential terrorist attack to mislead the voter into thinking the new WIV is necessary because otherwise terrorist attacks are certain to happen. This notion was taken over by other actors. Others, like Privacy First, go a step further, not only accusing the state of misleading the people, but of spreading fake news or lying. In this form, the delegitimization strategy is much more targeted at the government, or in general, at the actor trying to impose some security measure, than at the measure itself. Unlike the delegitimizing discourse that was aimed at the WIV itself, this form of delegitimizing discourse could be used as a main strategy for an actor (as it was in Lubach's March 2018 video), or it could be aimed at reaching a specific audience.

A good example of an audience that could be a good target for such a strategy would be the group of voters that feels a certain distance to or distrust in the state or government, like part of the people living in the north of the country, or people that vote for populist parties. As seen in the context chapter, there was a group of voters that said the main reason for them to vote against the WIV was because it was a form of protest in the government. Discourse that was aimed at delegitimizing the state or the governing parties would probably have been effective to reach this group of voters.

*Overview*

The expectations of this study were that at least part of the discourse coming from the opposers of the WIV would include desecuritizing, counter-securitizing or delegitimizing language. This was expected because the government, according to securitization theory, would otherwise be able to implement the new intelligence law uncontested. These expectations were partially found to be true. First, only counter-securitizing and delegitimizing resistance strategies were used by the opposers, as desecuritizing language would not be useful in this particular debate because there is a general consensus that terrorism is indeed a security issue.

Counter-securitizing language, and to a lesser extent delegitimizing language was not used by political parties and media throughout the whole political spectrum, but only by those on the left and right flanks. This means that this kind of discourse did not reach all voters, but that only the specific audiences of these left and right parties and media got influenced by it. It would then be expected that only people belonging to these groups would in majority vote against the WIV, but this not happen to be the case. Illustrative is the fact that 75% of both SP

voters and GL voters rejected the new intelligence law, although only SP used counter-securitizing language to convince its supporters to vote against the WIV. All in all, this study finds that resisting strategies could prove to be a helpful strategy in a debate on a securitized topic, but that they are not necessary to convince the public to reject a certain security measure.

*Implications of findings*

*Theoretical Implications*

First, the study has implications for the literature on securitization theory. Buzan et al. (1998) assume that when a subject has been move into the realm of security, governments have freedom to implement the measures they find necessary without experiencing too much political resistance. In this case, however, this did not turn out to be true. As explained in the above paragraphs, there is a consensus in society, even amongst opposers of the WIV, that terrorism is a serious security issue, and none of the opposers of the new intelligence law have tried to desecuritize the issue. Furthermore, only part of the opposing actors have used resistance tactics and only part of the public has been reached by these tactics, but still the majority of the public thought there were more cons than pros to this law, and the WIV was rejected. This means that the assumption that a government can implement any measure to fight a security matter is untrue. Furthermore, Buzan et al. (1998) write that once a topic is securitized, it is depoliticized. However, the fact that a referendum has been held on a security topic, and that the opposers of a security measure managed to convince the public to reject the measure without desecuritizing it could mean a topic could be both a security and a political topic.

The study also has implications for literature on resistance against securitization and, more specifically, counter-securitization. Only two major articles (Strilzel and Chang, Togpyal) have so far been written on this theory, and both papers were dealing with a specific case study, namely the war in Afghanistan and the Tibetan question. The case study used in this study is very different from these two. Firstly, both in the Afghanistan war and the Tibetan conflict there is actual violence (or even a war) going on, while the WIV debate was only about the threat of a potential attack in the Netherland, creating very different conditions. Also, in both case studies, the strategy of counter-securitization was used by the party that was being securitized by a (foreign) government, while in the WIV debate the two sides were arguing on a topic that was securitized. Despite these differences, the theory of counter-

securitization was still useful for this study, meaning the scope of the theory is larger than the case studies it had been used for so far.

The third scientific implication is that the theoretical definition of delegitimization can be changed so that it also includes strategies that question the integrity or credibility of an actor, as was done by some actors in the WIV debate. Also, arguments of necessity and proportionality were used relatively frequently, and these were also not included in the definition of delegitimization of Balzacq (2019), so they might also be an addition.

*Practical Implications*

On the practical side, it is difficult to determine what the implications of this study will be. Since both parties that have and have not made use of resistance tactics managed to get their supporters on board to vote against the WIV, it does not seem that parties will have to change their strategies. On the other hand, the fact that parties do not have to change their strategies according to this study might be interpreted as a confirmation of these strategies.

*Limitations*

Though this analysis allows us to see which political parties, NGOs and media made use of counter-securitizing and delegitimizing discourse to get their point across, it is not possible from this study for draw conclusion on whether such strategies were effective or not. Apart from the top-four reasons to vote against the WIV that was mentioned in the context chapter, little is known on the thought of voters on the WIV, meaning it is unknown whether voters followed the arguments of securitizing actors, and thus voted against the WIV because they perceived it to be a dangerous law. In order to establish the efficacy of certain resistance strategies, additional data on voter's motives and beliefs is necessary.

Furthermore, of a large part of the sources that were used in the research, it is not known how large the audience was that they reached, and of which people the audience consisted (age, education, political colour). This makes it difficult to estimate the weight an certain source should have in the discourse analysis. In this study, all sources were treated as if they had an equal weight, and quotes from sources that were probably not as visible to the public appeared in the analysis chapter just as often as quotes from very popular sources. Therefore, the extent to which the public has seen counter-securitizing and delegitimizing discourse appear in the debate might be different from what was described in the analysis.

The study did not include all the material that was available on the debate. Instead, a pre-selection of around 80 sources was made, of which around 40 were chosen, maintaining a maximum of two sources per actor (with the exception of Lubach). It might be the case that the sources that were not chosen from the pre-selection, or that were not found in the first place, contained a lot more securitizing or delegitimizing language than the sources that made it into the analysis, or that they did not include any of this kind of discourse. The results of the study could thus have been different, would the study have included all the sources with a certain minimum amount of views/reads. This was, however, not possible because of time constraints

Lastly, a discourse analysis always is a matter of interpretation. Another person might have interpreted some of the texts included in the research differently, leading to different results. In this study, the definitions of securitizing and delegitimizing discourse were set in the methodology section, making the analysis as accurate as possible, but it is not impossible that another researcher, using the same definitions, still would have considered some quotes now seen as securitizing not to be securitizing, or the other way around.

*Future research*

While this study confirms the presence of counter-securitization and delegitimization in the Dutch political debate, it does not say much about the effectiveness of such strategies, because of the lack of data on people's opinions on the issue. Future research could be done to another security-related political discussion, in which the resistance tactics used by the parties involved are analysed while also monitoring the reactions of the audience to such tactics. This could be done by consistently monitoring opinion polls, if they would include the right questions ("do you consider problem 'x' as a security threat?), or otherwise creating a survey.

Furthermore, the possibilities for using desecuritization as a resistance tactic should be submitted to further research. In the case study used in this thesis, there was no room for desecuritization since all the parties involved agreed on the fact that terrorism is indeed a security threat. There are other case studies, however, in which the topic that is being securitized is not accepted as a security threat by the whole population, creating leeway for political actors to do something with this strategy.

Cases that would be interesting to research in the future would be the current COVID-19 crisis, a topic that is seen as a security threat by a substantial part of the population and by the government, while there is also a large part of the population that believes the virus is not a

security threat. The climate crisis could eventually also grow into a case that could be interesting to research, as this is also a topic that part of the population views as an existential threat while others think its does not exist at all.

*Conclusion*

This study has proven that actors opposing the law on the intelligence- and security services have made use of resistance strategies against the securitization by proponents of this new law, such as the government. While desecuritization was not used by any actors, as all actors agreed on the fact that terrorism is a security issue, counter-securitization and delegitimization were used. Counter-securitizing strategies were used by actors located on both the left and the right flanks of the political spectrum, but not in the centre. A similar pattern could be discovered in delegitimizing strategies, though sometimes it was also used by actors in the political centre.

The main arguments used by opposers of the WIV were that it infringes on privacy and civil liberties, that the supervision on the services is insufficient, that the new law is not effective, and that the WIV allows the Dutch services to share data with their foreign counterparts too easily.

This study has theoretical implications for students of resistance tactics because it shows that counter-securitization is not only useful in conflict situations, but also in a normal political debate, and that theory on delegitimization can be expanded to include arguments aimed at discrediting an actor. Moving forward from this research project, knowledge on resistance tactics could be further increased by analysing the effectiveness of resistance strategies.

## References


Altena and van Atteveld (22 March 2018), Waarom stemde Noord-Nederland massaal 'tegen' bij het Wiv-referendum? *AVROTROS EenVandaag*, https://eenvandaag.avrotros.nl/item/waarom-stemde-noord-nederland-massaal-tegen-bij-het-wiv-referendum/

Babu-Kurra (2011, 11 September), *How 9/11 Completely Changed Surveillance in the U.S.* https://www.wired.com/2011/09/911-surveillance/

Balzacq, Thierry (2011). Securitization theory : How security problems emerge and dissolve. London [etc.]: Routledge.

Balzacq, Thierry (2015). Contesting Security: strategies and logic. London: Routledge

Balzacq, Thierry (2019). Securitization Theory: Past, Present, and Future. *Polity* 51(2), pp. 331-348

Behnke, Andreas (2006). No way out: desecuritisation, emancipation and the eternal return of the political. *Journal of International Relations and Development* 9, pp.62-69

Bolwijn, Marjon (2018, March 21). Voor de laatste twijfelaars: lees deze 25 vragen én antwoorden over het 'sleepwet'-referendum. *De Volkskrant*. https://www.volkskrant.nl/wetenschap/voor-de-laatste-twijfelaars-lees-deze-25-vragen-en-antwoorden-over-het-sleepwet-referendum~b5aaff59/

Buzan, B., Wæver, O., & Wilde, J. . (1998). Security: A new framework for analysis. Boulder, Colo: Lynne Rienner Pub.

Brakel, Rosamunde van, and Paul De Hert (2011). Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. *Cahiers Politiestudies* 20(3), pp. 165-194

Chalk, Peter (1998), The Response to Terrorism as a Threat to Liberal Democracy, *Australian Journal of Politics and History* 44(3), 373-388.

Crelinsten, R. (1998). The Discourse and Practice of Counter-Terrorism in Liberal Democracies. Australian Journal of Politics & History, 44(3), 389-413.

Croft, S. (2012). Securitizing Islam: Identity and the Search for Security. Cambridge: Cambridge University Press

Dragu, Tiberiu (2011), Is There a Trade-off between Security and Liberty? Executibe Bias, Privacy Protections, and Terrorism Prevention. *American Political Science Review* 105(1), 64-78

Ejdus, Bozovic (2017), Grammar, context and power: securitization of the 2010 Belgrade Pride Parade. *Southeast European and Black Sea Studies* 17(1), 17-34

Engelmann, Sabrina (2012). Barking Up the Wrong Tree: Why Counterterrorism Cannot Be a Defense of Democracy, *Democracy and Security* 8(2), 164-174

Fisher, K. (2011). Terrorist Threat Construction and the Transition to Permanent British Counterterrorism Law. Contemporary Voices: St Andrews Journal of International Relations, 2(3)

Gilley, Bruce (2009), The Right to Rule: How States Win and Lose Legitimacy. New York: Columbia University Press

Graaf, Beatrice de, and Eijkman, Quirine (2011). Terrorismebestrijding en Securitisering. *Justitiele Verkenningen* 37(8), pp.33-52

Gray, David (2017), *The Fourth Amendment in an Age of Surveillance*, Cambridge: Cambridge University Press

Hansen, Lene. 2006. Security as practice: discourse analysis and the Bosnian War. London: Routledge.

Jackson, Richard (2007) An analysis of EU counterterrorism discourse post-September 11, Cambridge Review of International Affairs, 20:2, 233-247

Jacobs et al. (2018), Het Wiv-referendum: Nationaal Referendum Onderzoek 2018, *Kennis Openbaar Bestuur*, https://kennisopenbaarbestuur.nl/media/255931/wiv-referendumonderzoek-2018.pdf

Kaunert, Christian & Sarah Léonard (2019) The collective securitisation of terrorism in the European Union, West European Politics, 42:2, 261-277

Kiesraad (2018), Nationaal referendum 21 maart 2018 https://www.verkiezingsuitslagen.nl/verkiezingen/detail/NR20180321

Leeuw, Jules van der (9 Oct 2018), Voldoende handtekeningen voor referendum over Sleepwet, *Algemeen Dagblad*, https://www.ad.nl/binnenland/voldoende-handtekeningen-voor-referendum-over-sleepwet~a17ff7ee/

MacAskill, Ewen and Gabriel Dance (2013, November 1). *NSA Files: Decoded*. The Guardian https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

Macnish, Kevin (2015). An Eye for an Eye: Proportionality and Surveillance. *Ethic Theory Moral Prac* 18, pp. 529–548

Marx, Gary T. (2015). Security and surveillance contests. In T. Balzacq: *Contesting Security: strategies and logic*. (pp.15-28). London: Routledge

Meijer, Remco and Frank Hendrickx (28 Oct 2017), Buma: Kabinet zal 'nee' bij referendum over 'de sleepwet' negeren, *De Volkskrant*, https://www.volkskrant.nl/nieuws-achtergrond/buma-kabinet-zal-nee-bij-referendum-over-de-sleepwet-negeren~bde660be/

Miles, Bart (2010). Discourse Analysis. In Neil J. Salkind, *Encyclopedia of Research Methods*, p. 368-370. Sage.

NOS (2018) Eindstand referendum: meer kiezers tegen inlichtingenwet dan voor. https://nos.nl/artikel/2223978-eindstand-referendum-meer-kiezers-tegen-inlichtingenwet-dan-voor.html

NOS Nieuws (2 Januari 2018). 125 Jaar de Telegraaf: “Je bent ervoor of ertegen”. *NOS* https://nos.nl/artikel/2210217-125-jaar-de-telegraaf-je-bent-ervoor-of-ertegen.html

Olesker, Ronnie (2018). The securitisation dilemma: legitimacy in securitisation studies, *Critical Studies on Security* 6(3), pp.312-329

Ollongren, K.H. (2017, December 15). Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017) en regeerakkoord [*letter to parliament*]. https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2017Z18166&did=2017D37427

Pantazis, Christina and Pemberton, Simon (2013). Resisting the advance of the security state: The impact of frameworks of resistance on the UK'S securitisation agenda. *International Journal of Law, Crime and Justice* 41, pp.358-374

Paternotte, Bas (29 Oct 2017), Bassiehof - Schoenen, Sleepwet & Sybrand, *GeenStijl*, https://www.geenstijl.nl/5139151/bassiehof-schoenen-sleepwet-sybrand/

Referendumcommissie (2018), Veelgestelde vragen over de WIV 2017 en het referendum van 21 maart 2018

Pilecki, Andrew, Jonathan M. Muro, Phillip L. Hammack, and Carley M. Clemons (2014). Moral Exclusion and the Justification of U.S. Counterterrorism Strategy: Bush, Obama, and the Terrorist Enemy Figure. Peace and Conflict: Journal of Peace Psychology 20(3), 285–299

Pol, Geart van der, et al. (2018), De 'Sleepnetwet' uitgelegd in 12 heldere vragen en antwoorden, *De Volkskrant*, https://www.volkskrant.nl/kijkverder/2017/sleepnet/

Richards, Neil (2013). The Dangers of Surveillance. *Harvard Law Review* 126, p.1934-1965

Schellevis, Joost and Rosalie Herderschee (22 March 2018). Wie stemde wat bij het referendum over de inlichtingenwet? *NOS* https://nos.nl/collectie/13642/artikel/2223858-wie-stemde-wat-bij-het-referendum-over-de-inlichtingenwet

Stritzel, Holger (2014). *Security in Translation: Securitization Theory and the Localization of Threat.* London: Palgrave Macmillan

Stritzel, Holger and Sean C. Chang. (2015) "Securitization and counter-securitization in Afghanistan." 47 Security Dialogue 46(6): 548-567.

Topgyal, Tsering (2016). The Tibetan Self-Immolations as Counter-Securitization: Towards an Inter-Unit Theory of Securitization. *Asian Security* 12(3), pp.166-187

Trombetta, M. (2008). Environmental security and climate change: analysing the discourse, *Cambridge Review of International Affairs* 21(4), pp.585-602.

Tweede Kamer (2016, 28 October), *Wet op de Inlichtingen- en Veiligheidsdiensten*, https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A34588

Vuori, Juha A. (2011). Religion Bites: Falungong, securitization/desecuritisation in the People's Republic of China. In T. Balzacq: *Securitization theory: How security problems emerge and dissolve*. (pp.182-211): London: Routledge

Vuori, Juha A. (2015). Contesting and Resisting Security in post-Mao China. In T. Balzacq: *Contesting Security: strategies and logic.* (pp.29-43). London: Routledge

Waltz, Kenneth N (1979). Theory of International Politics. Reading MA: Addison-Wesley Pub. Co.

Wright, D., & Kreissl, R. (Eds.). (2014). Surveillance in Europe. London: Routledge.

**Sources used for the analysis:**


Amnesty International (unknown). Sleepwet bedreiging voor mensenrechten. Consulted 5 April 2020 https://www.amnesty.nl/mensenrechten-in-nederland/veiligheid-en-mensenrechten/sleepwet

AVROTROS Een Vandaag (21 March 2018). Initiatiefnemers refendum: Iedereen heeft het over Sleepwet! https://eenvandaag.avrotros.nl/item/initiatiefnemers-referendum-iedereen-heeft-het-over-sleepwet/

AVROTROS Radar (25 September 2017). Sleepnetwet: Bestaat privacy straks nog wel? https://radar.avrotros.nl/uitzendingen/gemist/item/sleepnetwet-bestaat-privacy-straks-nog-wel/

AVROTROS Radar (5 March 2018). Het debat over de sleepwet. https://radar.avrotros.nl/uitzendingen/gemist/item/het-debat-over-de-sleepwet/

Bits of Freedom (unknown). Een betere wet. Consulted 5 April 2020 https://www.eenbeterewet.nl/wiv-referendum/index.html

Buitenweg, Kathalijne (1 March 2018). Waarom GroenLinks tegen de sleepwet is, *GroenLinks,* https://www.youtube.com/watch?v=hJRBuS7g_iE&feature=youtu.be

College voor de Rechten van de Mens (7 February 2017). Nieuwe wet op de inlichtingen- en veiligheidsdiensten: onvoldoende balans tussen veiligheid en privacy https://www.mensenrechten.nl/nl/nieuws/nieuwe-wet-op-de-inlichtingen-en-veiligheidsdiensten-onvoldoende-balans-tussen-veiligheid-0

Dijken, Jonathan van (16 March 2018). Sleepwet? What the FAQ?. *Piratenpartij*. Consulted 4 April 2020 https://piratenpartij.nl/sleepwet-what-the-faq/

Free Press Unlimited (12 September 2017). 3 redenen waarom het sleepnet slecht is voor de journalistiek. Consulted 5 April 2020 https://www.freepressunlimited.org/nl/nieuws/3-redenen-waarom-het-sleepnet-slecht-is-voor-de-journalistiek

Forum voor Democratie (8 October 2017). Bescherm uw privacy, teken nu voor referendum sleepwet. https://forumvoordemocratie.nl/actueel/oproep-baudet-teken-referendum-sleepwet

Gijzen, Marlou (15 March 2018). Als op zo'n manier grote groepen mensen worden doorzocht, zijn wij dan nog wel onschuldig totdat het tegendeel is bewezen? *De Volkskrant*

Graaf, Jelle de (7 October 2017). Red de democratie, stop de Sleepwet! *Joop!*. https://joop.bnnvara.nl/opinies/red-de-democratie-stop-de-sleepwet

GroenLinks (15 March 2018). Word wakker zonder de sleepwet. https://www.youtube.com/watch?v=KACpl3Gu1JU&feature=youtu.be

Hijink, Marc (20 March 2018). Het wordt 'Nee', die wet kan beter. *NRC Handelsblad*

Hoepman, Jaap-Henk (26 August 2017). Teken tegen de Sleepwet! *Het Financieele Dagblad*

Hoogland, Rob (20 March 2018). Big Brother. *De Telegraaf*

Horst, Han van der (14 March 2018). Ollongren vertelt u zelf waarom u tegen de sleepwet moet stemmen. *Joop!*. https://joop.bnnvara.nl/opinies/ollongren-vertelt-zelf-waarom-u-tegen-de-sleepwet-moet-stemmen

Martijn, Maurits (20 March 2018). Waarom ik tegen de nieuwe wet voor de geheime diensten stem. *De Correspondent*

Nieuwesteeg, Bernold (15 March 2018). Ineffectiviteit van Sleepwet is de laatste strohlam voor de tegenstanders. *Het Financieele Dagblad*

Noll, Cornelius (19 September 2017). 5 redenen waarom je tegen de sleepwet moet stemmen. *VICE*. https://www.vice.com/nl/article/kz7wny/5-redenen-om-het-sleepwetreferendum-te-ondertekenen

Noll, Cornelius (12 December 2017). Sleepwet gaat speurwerk alleen maar onoverzichtelijker maken. *VICE* https://www.vice.com/nl/article/vbzbj9/de-sleepwet-gaat-speurwerk-alleen-maar-onoverzichtelijker-maken

NOS/NTR Nieuwsuur (10 October 2017). De 'Sleepwet'. https://www.facebook.com/watch/?v=1654434154601448

Partij voor de Dieren (unknown). Massale bespieding via Sleepwet! Consulted 4 April 2020 https://www.partijvoordedieren.nl/standpunten/zeg-nee-tegen-massale-bespieding-via-sleepwet

Partij voor de Dieren (10 March 2018). Zeg NEE tegen de Sleepwet! https://www.facebook.com/watch/?v=1799964456722940

Piratenpartij – PPNL (30 January 2018). De Sleepwet: de vernieuwde Wet op de inlichtingen- en veiligheidsdiensten. https://www.youtube.com/watch?v=5eCISzq87wU

Privacy First (13 March 2018). ABC tegen de sleepwet. Consulted 5 April 2020 https://www.privacyfirst.nl/aandachtsvelden/sleepwet/item/1108-abc-tegen-de-sleepwet.html

Raak, Ronald van (February 2018). De Sleepwet is onnodig en gevaarlijk. *Socialistische Partij*. Consulted 4 April 2020 https://www.sp.nl/achtergrond/sleepwet-is-onnodig-en-gevaarlijk

Rooijendijk, Lotte (10 October 2017). Sleepwet tast bronbescherming aan en schrikt potentiële klokkenluiders af. *Transparency International*. Consulted 5 April 2020 https://www.transparency.nl/nieuws/2017/10/sleepwet-tast-bronbescherming-aan-en-schrikt-klokkenluiders-af/

RTL Entertainment (27 February 2018). Waar kan het misgaan met de eventuele sleepwet? – 5 UUR LIVE. https://www.youtube.com/watch?v=-ydsKYo5B4M

Rosman, Cyriel (17 March 2018). Als mensen 'voor' stemmen uit angst voor terreur, hebben wij het niet goed gedaan. *Algemeen Dagblad*

Rumulova, Adriana, Anouk Ruhaak, Saskia Naafs (15 March 2018). Een nog grotere hooiberg bouwen boven op een speld; onderzoek de nadelige gevolgen van de 'sleepwet'. *De Groene Amsterdammer*

Schaik, Lysanne van and Kevin Brongers (29 January 2018). Opinie: AIVD-succes maakt sleepwet overbodig. *De Volkskrant*

Socialistische Partij (February 2018). In anderhalve minuut waarom de SP tegen de sleepwet is. https://vimeo.com/258817390

Van Rossem (14 March 2018). Nederlanders zijn Sleepwetschapen. *GeenStijl*. https://www.geenstijl.nl/5141147/schapenleving/

Van Rossem (21 September 2017). Privacy Barometer: De sleepwet is niet effectief, intimiderend en onrechtmatig. *GeenStijl*. https://www.geenstijl.nl/5138591/teken-dan/

VPRO Buitenhof (4 March 2018). Referendum over de Sleepwet. https://www.vpro.nl/buitenhof/kijk/afleveringen/2018/Buitenhof-4-maart-2018.html

VPRO Zondag met Lubach (1 October 2017). Sleepwet https://www.youtube.com/watch?v=plLyjO0Qt7k

VPRO Zondag met Lubach (5 November 2017). Sleepwet #2 https://www.youtube.com/watch?v=SdASXiLdOzk

VPRO Zondag met Lubach (18 March 2018). Referendum over de WIV https://www.youtube.com/watch?v=XoCMkJbcYUM

Wijnberg, Rob (20 March 2018). Waarom de zuch naar méér inlichtingen nooit zal ophouden (en ik dus 'tegen' stem bij het referendum). *De Correspondent*

Winter, Leon de (20 March 2018). Nog even, en Orwell's 1984 is een feit. *De Telegraaf.*

## Appendix

*Color Codes:*

Arguments:

WIV infringes on privacy and/or civil liberties

Chilling effect

Protection of journalistic sources

Sharing of data with foreign services

WIV will not be effective

Future government / leaders

Retention term is too long

Resistance Tactics:

Counter-securitization

Desecuritization

Delegitimization

**Waarom GroenLinks tegen de sleepwet is (Speech MP Kathalijne Buitenweg, 1 maart 2018**

Introductie > (…) > En laat ik mijn vier belangrijkste redenen noemen.

En de eerste is de bron, is eigenlijk de kern van alle problemen, en dat is de sleepnetbevoegdheid (…)

Het sleepnet dat is het massaal en ongericht verzamelen van gegevens, om pas later te kijken wat je ermee gaat doen. Denk aan het slepen van al het internetverkeer van een wijk. En zo'n sleepnet raakt ons dus allemaal, ook onschuldige burgers. Met wie we appen, met wie we bellen, welke sites we bezoeken, het kan allemaal als bijvangst bij de diensten worden binnengehaald en opgeslagen.

Maar was is daar nou erg aan? Zullen de voorstanders zeggen. Nou wat heb ik te verbergen?

Nou dat zal ik zeggen: de kern van wie ik ben. Een individu in een vrije samenleving. Want als je weet dat de overheid je altijd kan volgen, als je merkt dat de overheid meekijkt, dan heeft dat een effect op je gedrag. Bewust of onbewust zullen velen rekening houden met wat ze schrijven. Welke artikelen ze lezen, en welke reisschema's ze plannen. Massale surveillance van ons allemaal dat gaat ten koste van de creatieve samenleving. Dat gaat ten koste van onze innovatieve economie. En dan verliezen we een stuk van onze vrijheid.

De essentie van het sleepnet is dat het alles binnenharkt. Binnensleept. En daar zitten dus ook gegevens bij die in Nederland eigenlijk beschermd zijn. Dat is mijn tweede probleem met deze wet. Het ondermijnt bijvoorbeeld de bronbescherming van Journalisten. En die is belangrijk om misstanden aan het licht te krijgen. En het is niet voor niets dat ook de NVJ, de Nederlandse Vereniging van Journalisten, buitengewoon kritisch is.

Laat ik een voorbeeld geven. Als de geheime diensten een sleepnet leggen om de Amsterdamse wijk Wittenburg, dan raakt dat ook de redacties van het Parool, de Volkskrant en Trouw. En als je in deze hooiberg van data dan gaat zoeken naar contacten van mensen met Rusland, dan hoor je niet alleen het hoongelach over Poetin's datsja, maar dan zie je misschien ook de bron van de journalistike scoop.

En dat brengt me bij probeem drie: de samenwerking met buitenlandse diensten. De berg gegevens die van Nederlandse burgers wordt verzameld, die mag ongelezen worden doorgegeven aan buitenlandse diensten, als in een soort zwarte doos. En ja, daar kunnen dus ook journalistieke bronnen tussen zitten. Of uitspraken van mensen die kritisch zijn op Erdogan. Of bedrijfsgeheimen die voor de Amerikaanse concurrent interessant zijn. Of medische informatie die verzekeringsmaatschappijen dolgraag willen zien. Het doorsluizen van ongelezen data, daar moeten we een streep doorhalen.

Maar beste GroenLinksers, ik heb ook goed nieuws. Want de minister heeft gezegd dat het massaal en ongericht afluisteren niet de bedoeling is. Het kan wel, maar ze zullen het niet doen. Of anders: niet vaak. En er komst zelfs een heuse evaluatie om ervoor te zorgen dat de diensten hun bevoegdheden niet volledig zullen gebruiken – of anders niet te vaak. Is dat niet bizar? Dat de grenzen aan de macht van de geheime diensten op beloftes hangen? Dat die in een regeerakkoord staan? Die garanties, die moeten in de wet zelf ! Want vooruit, ik wil minister Ollongren best of haar blauwe ogen geloven, maar wie zit er na haar aan de knoppen? Als de bevoegdheden van de diensten in de wet zijn vastgelegd, dan moeten de grenzen daaraan in dezelfde wet zijn geregeld.

En die grenzen die zullen de wet juist sterken maken, niet zwakker. Want opsporing dat moest juist gericht gebeuren. Zoals Oud-NSA-directeur Bill Binney zei: "Bulkdata kills people" Een sleepnet levert teveel gegevens op. Als we de hooiberg kleiner maken vinden we eerder de speld en dan zetten we in op vrijheid én veiligheid. En beste mensen, daarom is GroenLinks tegen de sleepwet. We willen af van het sleepnet. We willen dat journalisten hun bronnen kunnen beschermen. We willen weten wat we aan buitenlandse diensten geven en we willen dat garanties in de wet worden vastgelegd. Deze wet moet worden herschreven. Dat vind ik en ik heb het van velen van jullie gehoord. Daar gaan we samen zoveel mogelijk anderen overtuigen. Op 21 maart laten we van ons horen tegen de sleepwet, en voor vrije mensen.

**GroenLinks: Word wakker zonder de sleepwet (video)**

Beschrijving: Al je mailtjes, chats en belletjes kunnen straks blijven hangen in het sleepnet van de geheime diensten. Klink eng, hè? Vinden wij ook. Word wakker zonder de sleepwet. Stem op 21 maart tegen.

Video zonder tekst. Toont mannetje van geheime dienst die meekijkt met persoonlijke communicatie

**Forum voor Democratie "Bescherm uw privacy, teken nu voor referendum sleepwet" 8 oktober 2017**

(onheilspellende muziek)

Je e-mails, je Whatsappjes, je internet zoekgeschiedenis. Je telefoongesprekken. Wie je vrienden zijn, met wie je aan het daten bent, je elektronisch patiëntendossier, en dat je stiekem op zoek bent naar een andere baan.

Al dat soort zaken kan de overheid straks zonder enig probleem bekijken en jarenlang opslaan en bewaren als je nieuwe wet op de inlichtingen- en veiligheidsdiensten erdoor komt.

De sleepnetwet wordt die genoemd, omdat ie als een sleepnet alle mogelijke informatie kan verzamelen, ook informatie die niets met een strafbaar feit te maken heeft.

Big Brother will be watching you.

Maar hebben wij daar niet ook nog iets over te zeggen? Moeten wij daar niet een debat over voeren met elkaar? Het onderwerp is nauwelijks aan bod gekomen in de verkiezingscampagnes, toch wordt deze wet er nu zomaar doorheen gejast. Wij vinden dat het hoog tijd is voor een referendum. Ga naar www.sleepwet.nl en teken.

Want als wij niet voor onze privacy opkomen, raken wij die onmiddellijk kwijt.

**SP: De Sleepwet is onnodig en gevaarlijk.**

DE SLEEPWET IS ONNODIG EN GEVAARLIJK

Tegelijk met de gemeenteraadsverkiezingen vindt op 21 maart het referendum plaats over de nieuwe Wet op de inlichtingen- en veiligheidsdiensten, beter bekend als de Sleepwet. Dat het raadgevend referendum doorgaat is bijzonder, aangezien VVD, CDA, D66 en ChristenUnie in het regeerakkoord besloten hebben om het af te schaffen. Bovendien hebben deze partijen al laten weten dat de Sleepwet er hoe dan ook gaat komen. De overheid wil je wel afluisteren, maar niet naar je luisteren, zo lijkt het.

Aanslagen voorkomen doe je door gericht terroristen te volgen en geradicaliseerde salafistische netwerken te ontmantelen, het met een ‘sleepnet’ massaal binnenhalen van gegevens van onschuldige burgers helpt daarbij niet. Informatie van alle Nederlanders kan straks worden gedeeld met de geheime diensten van andere landen, ook gegevens die helemaal niet zijn geanalyseerd en waarvan we dus ook niet weten of die tegen onze burgers kunnen worden gebruikt. De nieuwe wet op de geheime diensten gaat gelden voor alle mogelijke technologieën die in de toekomst worden ontwikkeld, zonder dat de Tweede Kamer dat weet of daarvan op de hoogte wordt gebracht.

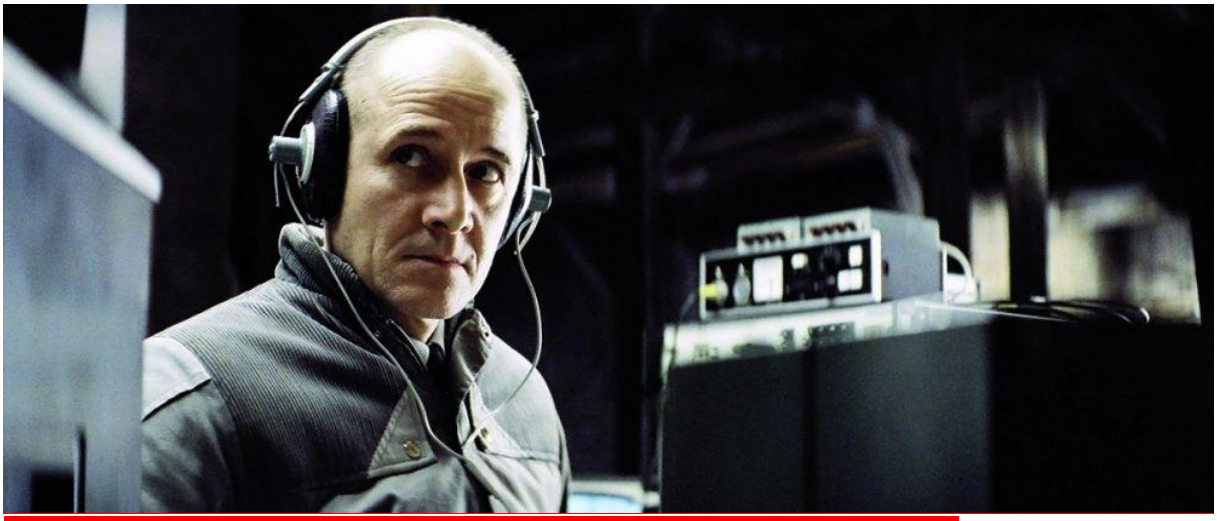
Dit zijn enkele argumenten tegen de Sleepwet, een wet die volgens het kabinet geen ‘Sleepwet’ mag heten. Bij het opstellen van de wet sprak de regering van ‘ongerichte kabel-gebonden interceptie’, dat is massaal verzamelen van gegevens van burgers. Maar omdat dit niet erg populair klinkt, maakte toenmalig PvdA-minister Plasterk daar maar ‘doelgericht’ van. Na een kritische internet-consultatie werd het plotseling wéér anders: een ‘onderzoeks-opdracht-gerichte interceptie’. Dit is gegoochel met woorden, wat moet verdoezelen wat deze wet in werkelijkheid is: namelijk gewoon een ‘Sleepwet’.

Trap niet in de terreurschwalbe

In het debat over de regeringsverklaring in november werd al duidelijk wat in maart de strategie is van de regeringspartijen in het referendum over de nieuwe Sleepwet. Zij willen niet zozeer een discussie voeren over de noodzaak en effectiviteit van deze wet, maar zullen vooral proberen tegenstanders verdacht te maken: als je vóór dit referendum bent, zou je ook verantwoordelijk zijn voor aanslagen. Arjen Lubach muntte voor deze houding in zijn tv-programma de prachtige term ‘terreurschwalbe’. Het is maar zeer de vraag of het massaal binnenhalen van gegevens van onschuldige burgers noodzakelijk en effectief is voor het voorkomen van aanslagen en het bestrijden van terrorisme. Die discussie heeft de SP ook in de Tweede Kamer proberen te voeren, tijdens de behandeling in februari van de nieuwe wet voor de geheime diensten, waar het nieuwe ‘sleepnet’ een onderdeel van is. Die discussie bleek moeilijk, omdat de woordvoerders van de meeste partijen zich ook hier beperkten tot terreurschwalbes. Opmerkelijk is de rol van D66. Tweede Kamerlid Kees Verhoeven voerde destijds samen met ons oppositie tegen deze wet en diende zelfs een amendement in om de ‘sleepfunctie’ uit deze wet te halen. In maart zal D66 echter campagne gaan voeren vóór de Sleepwet.

De FBI gelooft het ook niet

De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) waarschuwde vorig jaar dat het doorzoeken van massa's gegevens van onschuldige burgers niet effectief is voor de bestrijding van terreur: 'Omdat elke terroristische aanslag uniek is, is het nagenoeg onmogelijk om een goed profiel te maken.' In de Verenigde Staten heeft de geheime dienst NSA al jarenlang ervaring met het massaal binnenhalen van gegevens van burgers, maar ook daar groeide de kritiek. De FBI moest na een onderzoek toegeven dat de werkwijze van de NSA niet bewijsbaar heeft bijgedragen aan het voorkomen van aanslagen. Hoogleraar Beatrice de Graaf – een vooraanstaand lid van de ChristenUnie – stelt dat je terrorisme niet zozeer bestrijdt met data, maar vooral met mensen. Of wat te denken van onderzoek van de Raad van Europa, onder leiding van CDA-Kamerlid Pieter Omtzigt? Dat bevestigt nogmaals dat uit onafhankelijk onderzoek in de VS is gebleken dat dit soort massasurveillance 'vermoedelijk niet heeft bijgedragen aan het voorkomen van terroristische aanslagen, in tegenstelling tot hetgeen werd beweerd door hoge inlichtingenofficieren'. Tijd voor het CDA om toch eens naar Pieter Omtzigt te luisteren.



Zit de overheid straks bij ons op zolder, zoals in de film Das Leben der Anderen? Still: Everett Collection, Inc.©

Ze kunnen straks altijd meekijken

Het Internet of Things – het internet der dingen – biedt in de toekomst veel mogelijkheden, om problemen op te lossen en ons leven gemakkelijker te maken. Maar deze nieuwe technologieën bieden ook ongekende mogelijkheden voor afluisteren en spionage. En om te hacken. Je auto bijvoorbeeld, als je onderweg bent, of je telefoon, als je thuis bent – en in theorie kan zelfs je pacemaker worden gehackt. Geheime diensten kunnen straks meekijken en meeluisteren als je aan het mailen bent of aan het daten. Of als je met je geliefde belt, of bankzaken doet, of gewoon een computerspelletje speelt. Ook als je zelf niet met je computer of je telefoon werkt, kunnen deze door anderen als een camera of microfoon worden gebruikt. Ook chips in het lichaam kunnen in de toekomst worden gehackt.

Elke hack is een toegangspoort

De nieuwe wet voor de geheime diensten is 'techniek onafhankelijk'. Bewust is niet opgenomen op welke technologieën de geheime diensten allemaal mogen inbreken. Dat is wel zo gemakkelijk, omdat de wet dan bij nieuwe ontwikkelingen niet steeds opnieuw hoeft te worden aangepast. Maar het is tegelijk ook gevaarlijk, want de geheime diensten kunnen in de toekomst van alles gaan doen. Denk aan hacken. Dat kan heel gericht bij verdachte personen, maar evengoed bij onschuldige burgers en bij alle dingen die verbonden zijn met internet. Dit kan een effectief middel zijn voor geheime diensten, in de strijd tegen potentiële terroristen. Maar de hack van de één is ook een poort voor de ander. De AIVD en de MIVD maken gebruik van zwakheden in informatiesystemen, maar de vraag is natuurlijk of zij die zwakheden niet juist zouden moeten melden, zodat burgers en bedrijven zich zo goed mogelijk kunnen beveiligen.

Informatie alsnog witwassen

Als de AIVD en de MIVD straks massaal informatie gaan opslaan, kunnen deze gegevens alleen op een geautomatiseerde wijze worden verwerkt. Dat gebeurt met behulp van modellen en algoritmen, die patronen en profielen maken. Deze analyses geven correlaties, maar geen causaliteit. Mensen lopen de kans dat over hen allerlei conclusies worden getrokken, zonder dat naar hun persoonlijke omstandigheden wordt gekeken. Het houden van toezicht op dit soort geautomatiseerde processen kan ook alleen op een geautomatiseerde wijze. Een soort 'meta-toezicht' op processen, maar niet op de gevolgen voor personen. Nog groter is het probleem als onze geheime diensten niet-geëvalueerde data gaan delen met geheime diensten uit andere landen.

We weten dan niet meer wat voor soort gegevens worden gedeeld en we weten ook niet wat voor soort bewerkingen worden gedaan – en wat voor maatregelen op basis daarvan worden genomen. Maar dat gebeurt wel met gegevens die onze diensten hebben verzameld over onze eigen burgers. Data die vervolgens door andere diensten weer kunnen worden gedeeld met de AIVD en de MIVD. Ook informatie die onze diensten volgens onze wet helemaal niet zouden mogen hebben.

Kunnen we Trump vertrouwen?

De nieuwe wet gaat over de regels die wij stellen voor onze geheime diensten. Maar het allergrootste gevaar komt uit landen als Rusland of China, Israël of Iran. Maar ook uit de Verenigde Staten, waar president Trump zich heel weinig zal aantrekken van welke wet die wij hier ook maken. In de wereld van de geheime diensten gelden niet zozeer wetten en regels, maar vooral macht en tegenmacht. Dat geldt voor oude vijanden, maar helaas ook nog steeds voor vermeende vrienden. In april 2014 werd er in de Tweede Kamer op mijn initiatief een debat gevoerd naar aanleiding van de onthullingen van Edward Snowden. Dat was een ongemakkelijk debat, omdat de minister telkens sprak over de bescherming van onze burgers tegen onze geheime diensten. Maar het allergrootste gevaar dat burgers lopen komt niet van de AIVD of de MIVD, maar van het optreden van buitenlandse diensten. Met wie wij massaal gegevens gaan delen van onze eigen mensen, informatie die wij niet eens hebben kunnen analyseren en waarvan we helemaal niet weten wat erin staat. In maart spreken we over nut en noodzaak van de nieuwe Sleepwet. Maar we moeten het ook hebben over de bescherming van onze burgers. Kunnen we erop vertrouwen dat Trump fatsoenlijk omgaat met gegevens van onze mensen?

**In anderhalve minuut waarom de SP tegen de Sleepwet is.**

Op 21 maart vindt het referendum plaats over de Sleepwet, de nieuwe wet op de inlichtingen- en veiligheidsdiensten. Om terrorisme te bestrijden zou onze geheime dienst, de AIVD, meer bevoegdheden moeten krijgen, zoals het op grote schaal afluisteren van mensen.

We moeten alles doen om aanslagen te voorkomen, maar het op grote schaal verzamelen van gegevens van onschuldige mensen gaat daarbij niet helpen. Want in plaats van de hooiberg groter te maken, kan je beter gericht zoeken naar de speld!

Vaak zien we dat aanslagplegers al in beeld waren bij veiligheidsdiensten ergens in Europa. De geheime diensten moeten informatie over verdachten veel beter delen. Radicalisering moeten we voorkomen, en haatzaaiers moeten worden aangepakt.

Maar de AIVD kan straks op grote schaal informatie van onschuldige mensen verzamelen, ook van artsen, advocaten en journalisten. Deze informatie mag worden gedeeld met andere landen, zonder dat de AIVD weet welke informatie dit is, en zonder te weten wat die landen met al die gegevens van Nederlanders gaan doen

(Jan heeft een belastingschuld – Rachid is homoseksueel – Karel heeft syfilis)

Ook mogen geheime diensten alle technologieën gebruiken om af te luisteren of te hacken, van je smartphone tot aan je zelfrijdende auto bijvoorbeeld.

Het referendum is een middel voor mensen om politici terug te fluiten als die besluiten nemen die ze helemaal niet willen. De regering wil het referendum afschaffen. Ze zeggen dat de sleepwet er toch moet komen.

(verder over referendum)

**Massale Bespieding via Sleepwet! – PvdD, ongedateerd**

**In juli 2017 is in Nederland de sleepwet aangenomen. Deze wet zorgt ervoor dat zonder enige aanwijzing iedere burger mag worden afgetapt. Onder het mom van terrorismebestrijding wordt de sleepnet-methode ingevoerd: grote hoeveelheden willekeurige gegevens worden verzameld en doorzocht op patronen. Onnodig, want uit onderzoek naar aanslagplegers bleek dat zij allang in beeld waren bij de geheime diensten. De PvdD heeft in de Tweede en Eerste Kamer tegen deze sleepwet gestemd.**

Mensen brengen steeds meer tijd online door. De mobiele telefoon, de tablet of de computer is steeds binnen handbereik. Alles wat je doet, zegt, vindt, hebt of bent, waar je bent en met wie, is tegenwoordig online te vinden. En de overheid kijkt straks met je mee en slaat alles op voor drie jaar en misschien wel voor altijd.

Met de Wet op de inlichtingen- en veiligheidsdienst (WIV) 2017, ofwel de sleepwet, wordt iedere burger verdacht gemaakt en worden hun rechten ingeperkt. Voor de Partij voor de Dieren wordt met het in de gaten houden van onschuldige mensen een grens overschreden. Privacy biedt ons veiligheid en beschermt ons tegen de staat. Wanneer we onze privacy opgeven, geven we een belangrijk deel van onze veiligheid op. Inperking van de rechten van burgers mag alleen in uiterste gevallen.

De PvdD hecht veel waarde aan de privacy van burgers en vindt het daarom belangrijk dat zij zich kunnen uitspreken over deze omstreden wet, waarmee het internet grootschalig mag worden afgeluisterd door de geheime dienst.

**Medisch beroepsgeheim en journalistieke vrijheid**

De Partij voor de Dieren is fel tegenstander van de inwerkingtreding van deze sleepwet en herziening van de WIV in deze vorm. Maar dat betekent niet dat wij niet bereid zijn mee te werken aan een wet die wel goed is voor onze privacy en onze veiligheid wel dient. Op een aantal essentiële knelpunten hebben wij moties ingediend.
De Partij voor de Dieren heeft verzocht dat het medisch beroepsgeheim omhoog moet blijven en dat deze op dezelfde wijze behandeld moet worden als informatie van advocaten. De Partij voor de Dieren wil dat de medische informatie dus expliciet vrij wordt gesteld van verzameling en opslag door veiligheidsdiensten.
Daarnaast maakt de Partij voor de Dieren zich ernstig zorgen over de bronbescherming van journalisten. Onafhankelijke (onderzoeks-) journalistiek is noodzakelijk voor de controle op de macht en kan worden ingeperkt met de WIV.

De Partij voor de Dieren wil dat er een verbod wordt opgenomen voor het delen van ongeëvalueerde gegevens met buitenlandse inlichtingendiensten en daarom hebben wij de regering verzocht een

verbod op te nemen op het hacken van derden, tenzij zij in directe technische relatie staan tot het doelwit.

***Toezicht***

Wanneer de AIVD en de MIVD een "onderzoekopdrachtgerichte interceptie" aanvragen willen deze diensten, omdat ze nog onvoldoende kennis bezitten en dus niet gericht te werk kunnen gaan, alle telecommunicatie (online en offline) verwerven, verwerken en analyseren.

Om hier een voorstelling van te maken: De Noordzee ligt helemaal vol met data. De veiligheidsdiensten denken te weten dat ergens langs de Nederlandse kust belangrijke data te vinden is. Vervolgens gaan ze met een sleepnet langs de gehele Nederlandse kust in de hoop dat ene kleine stukje data te vangen. Alle bijvangst, de data van jou en van ons, mogen ze vervolgens 3 jaar op hun sleepboot laten liggen want wellicht hebben ze het nog een keer nodig. Of ze dat ene stukje data nou hebben gevonden of niet.

De minister krijgt een verzoek van de AIVD of MIVD om zo'n onderzoek op te starten. Wanneer de minister dit verzoek goedkeurt gaat deze vervolgens naar de TIB (toetsingscommissie). Zij moeten toestemming geven voordat de AIVD of MIVD het sleepnet gaan uitgooien. Deze commissie moet bestaan uit twee (oud) rechters en een technisch expert.

*Gezien de vaagheid van de wet en de onbeperkte mogelijkheden van de veiligheidsdiensten is het belangrijk dat de toetsingscommissie de reikwijdte bepaald. Doen zij dit niet of onvoldoende dan zal het sleepnet groter en groter worden.*

*Interessant detail: Er zijn geen drie maar slechts twee "geschikte" kandidaten voor de toetsingscommissie gevonden. Omdat de regering deze toetsingscommissie nodig heeft om de wet in werking te laten treden hebben ze genoegen genomen met deze twee kandidaten*. De Partij voor de Dieren ziet dat er nu al een loopje wordt genomen met het toezicht. De Partij voor de Dieren was de enige partij in de Tweede Kamer die tegen de benoeming van deze kandidaten heeft gestemd.

Wanneer de AIVD of de MIVD mogen beginnen met het uitgooien van hun sleepnet is er ook een extra toets van de CTIVD (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten) nodig. Wanneer de CTIVD opmerkt dat er iets niet klopt aan de aanvraag of de werkwijze, zullen ze dit doorgeven aan de regering en eventueel aanbevelingen doen. De regering moet vervolgens deze aanbevelingen doorsturen ter beoordeling aan de toetsingscommissie (die dus al de eerste toetsing gedaan heeft). De toetsingscommissie moet dus uiteindelijk beslissen of de toetsingscommissie zelf zijn werk wel goed gedaan heeft.

*De Partij voor de Dieren vindt dan ook de de CTIVD een bindend en onafhankelijk advies moet kunnen geven. Zoals de wet nu geformuleerd is zijn we onvoldoende beschermt tegen machtsmisbruik.*

**Zeg NEE tegen de sleepwet!**

De Partij voor de Dieren is van mening dat privacy veiligheid ís. Wij zullen nooit tolereren dat onze mensenrechten, onze grondrechten op het spel worden gezet voor schijnveiligheid.

**Zeg NEE tegen de sleepwet! (Video PvdD)**

Dit is Fleur. Fleur houdt van vrijheid, maar ook van veiligheid. Daarom heeft ze Rex, een heel waaks beestje. Maar Rex is onverzadigbaar. Rex eet Fleur de oren van het hoofd, en hij groeit haar ook een beetje boven het hoofd. Rex bewaakt en bespiedt Fleur, of zij dat nou wil of niet.

Hij doet niets hoor, wil alleen maar spelen. Maar, hij heeft wel een eigen willetje. Met de Sleepwet neemt Rex het helemaal over van Fleur. Geen fijn plan.

Voel je vrij om nee te stemmen, tegen de sleepwet, voor alle veiligheid.

(Rex is een T-rex, eet Fleur op in het filmpje)

**DENK: Waarom is Denk tegen de sleepwet?**

Hier in de Tweede Kamer worden wetten gemaakt. En die wetten zijn meestal goed voor Nederland. Maar de Sleepwet is dat niet. De sleepwet gaat veel te ver en tast onze burgerrechten aan. En waarom is dat zo? Als er iemand verdacht wordt in de omgeving waarin jij bent, dan mag de overheid alles aftappen waar informatie op staat. Op je ipad, telefoon, computer…

Die informatie die mogen ze delen met andere geheime diensten zonder dat ze de onschuldige mensen eruit halen. Wij vinden dat veel te ver gaan. Op 21 maart stemmen wij tegen de sleepwet.

Piratenpartij:

Er is een gevaarlijke wet op komst. Een bedreiging voor onze burgerrechten en de manier waarop we omgaan met communicatie. Ze noemen het de sleepwet, in de Piratenpartij is tegen.

De sleepwet geeft inlichtingen- en veiligheidsdiensten toestemming om massaal informatie af te luisteren en op te slaan.

Je telefoon, computer, tv, horloge, smartspeaker…

Als de wet doorgaat mogen ze wanneer één iemand ergens van wordt verdacht de gehele wijk afluisteren.

Onderzoek heeft aangetoond dat deze willekeurige manier van afluisteren niet effectief is tegen terrorisme. Ik ben voor gericht onderzoek.

In het voorstel staat dat verzamelde data doorgestuurd kan worden naar andere landen, zonder dat dat eerst wordt geanalyseerd. Fucking slecht.

In sommige landen wordt de bevolking 24/7 digitaal gecontroleerd. Deze wet is een stap in de verkeerde richting.

Wanneer je eigen veiligheidsdiensten je afluisteren, ben je niet meer vrij om te zeggen wat je vindt van je eigen overheid.

De sleepwet maakt tevens een DNA-databank legaal, en daarmee maken we genetisch profileren mogelijk. Zonder bewaartermijn, die gegevens gaan nooit meer weg.

*Zonder goed toezicht moet deze wet van tafel.*

Massasurveillance of jouw apparaten, in jouw huis, is in strijd met je recht op privacy, met de vrijheid van meningsuiting, met de vrijheid van godsdienst en levensovertuiging, met je recht op een eerlijk proces en je recht op een gelijkwaardige behandeling.

We hebben één kans om aan te geven dat wij dit niet willen in Nederland. Een stem tégen de sleepwet is een stem vóór een betere wet. Op 21 maart kan je stemmen tijdens het referendum, dus informeer jezelf, denk na en stem.

**Sleepwet? What the FAQ? – Piratenpartij**

Op 21 maart a.s. vindt het referendum plaats over de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017), ook wel bekend als de sleepwet. Voor of tegen stemmen? De Piratenpartij geeft een toelichting aan de hand van een aantal vragen en stellingnames. Informeer jezelf, denk na, en stem. De Piratenpartij wenst je veel wijsheid bij je keuze.

Q “Grootschalig aftappen is maar lastig: we moeten per glasvezel kijken wat we gaan doen!”

Dit klopt niet (helemaal); een tap kun je per glasvezel plaatsen, maar dit hoeft niet per se in een wijkcentrale plaats te vinden. Via een ‘internet backbone‘ (knooppunt) kun je relatief gemakkelijk niet enkel een glasvezel pakken, maar de data van alle vezels tegelijkertijd. Deze data filter je weer met speciale hard- en software, zodat je enkel het verkeer verwerkt dat je wilt ontvangen en waar je toestemming voor hebt gekregen (bijvoorbeeld al het verkeer uit een specifieke wijk of gebied). Technologie om dit mogelijk te maken bestaat tenminste sinds 2006. Zie hiervoor bijvoorbeeld de documentatie over ‘room 641A‘. Zo verkregen verkeer kan daarna automatisch geanalyseerd worden via het bestaande ARGO II systeem. Hier zal op basis van metadata en algoritmes een rapportage uit rollen. Deze metadata is dan vrij te gebruiken door de diensten.

Zo hoef je niet steeds per opdracht een nieuwe fysieke tap te plaatsen, maar is de beperking eerder softwarematig. Op dit moment is ARGO II middels een plugin begrensd om te voldoen aan Wiv 2002. Met de Wiv 2017 is ARGO II volledig inzetbaar. De enige technische beperking op de grootte van het aftappen is hoeveel geld we bereid zijn te betalen voor de data opslag en analyse.

Q “Advocaten zijn beter beschermd in Wiv 2017”

Via Artikel 28, 29, 30 en 66 van Wiv 2017 zullen advocaten inderdaad beter beschermd zijn tegen gericht aftappen. Gericht aftappen is dan enkel mogelijk met toestemming van de rechtbank in Den Haag. Echter kunnen de gegevens van een advocaat nog steeds wél meegesleept worden, mocht deze toevallig in een sleepnet terecht gekomen zijn, want ook een advocaat woont wel eens in de buurt van iemand die wordt onderzocht. Deze gegevens moeten dan eerst geanalyseerd worden om vast te stellen dat het gaat om gegevens van een advocaat. Hiermee zal de geheime dienst sowieso de metadata zien – deze heb je immers nodig om dit vast te stellen. Daarnaast bestaat er nog steeds de mogelijkheid dat deze gegevens ‘witgewassen‘ worden via een buitenlandse inlichtingendienst.

Q Journalisten worden toch ook beschermd?

Bronbescherming van journalisten is inderdaad afgeschermd: via artikel 28, 29 en 30 wordt er expliciet gesproken over het beschermen van bronnen van journalisten. Om hierop te mogen

onderzoeken is ook toestemming nodig van de rechtbank in Den Haag. Het is echter niet duidelijk wie wel of niet als journalist gezien wordt. Iedereen met een perskaart? Een student opleiding journalistiek? Iedereen in dienst van traditionele media? Ook kunnen gegevens van journalisten nog steeds meegesleept worden, mocht deze toevallig in een sleepnet terecht gekomen zijn door een onderzoeksopdrachtgerichte interceptie in de omgeving. Op basis van metadata is het snel duidelijk wie met wie praat. Zo is het ook snel duidelijk wie bijvoorbeeld als klokkenluider een maatschappelijke kwestie kenbaar wilde maken. Daarnaast bestaat er ook hier de mogelijkheid dat gegevens 'witgewassen' worden via een buitenlandse inlichtingendienst.

Q Medische gegevens dan?

Medische gegevens mogen niet zomaar gebruikt worden. Toch mag er gericht gezocht worden naar medische gegevens en mag de geheime dienst eventueel gericht infrastructuur hacken om medische gegevens buit te maken. Hierdoor is het medisch beroepsgeheim niet meer gegarandeerd. De AIVD geeft aan dat ze deze medische gegevens enkel zal gebruiken als dit absoluut noodzakelijk is als sluitstuk in een onderzoek. Garanties in wetgeving worden hier echter niet voor gegeven. Daarnaast bestaat er nog steeds de mogelijkheid dat deze gegevens 'witgewassen' worden via een buitenlandse inlichtingendienst.

Q Wat bedoel je met witwassen?

Binnen de Wiv 2017 is toegestaan dat de geheime dienst gegevens uitwisselt met andere buitenlandse geheime diensten zonder dat ze daar eerst een eigen analyse op hoeft te doen. Als buitenlandse geheime diensten vervolgens door onszelf verzamelde gegevens aan ons teruggeven, vindt er géén extra controle plaats of de verwerking hiervan aan onze eigen wet getoetst kan worden. Hierdoor bestaat er de mogelijkheid dat gegevens uit een eerste interceptie die niet binnen de Nederlandse wettelijke kaders vallen, alsnog door buitenlandse diensten geanalyseerd worden en uiteindelijk toch gebruikt worden door Nederlandse inlichtingendiensten. Een ingediend amendement om dit te beperken is weggestemd in de Tweede Kamer.

Q En het regeerakkoord?

Onze huidige regering heeft in haar regeerakkoord staan: "Van het willekeurig en massaal verzamelen van gegevens van burgers in Nederland of het buitenland ('sleepnet') kan, mag en zal geen sprake zijn." Voor de Piratenpartij leest dit als een intentieverklaring met een uitsluitend tijdelijke en politieke betekenis. Omdat er geen juridische waarde van uit gaat, vinden we dit onvoldoende. Het is ook van belang dit te verankeren in wetgeving, zodat dit ook geldt ná deze regering. Wiv 2017 staat een sleepnet expliciet toe. We moeten er dus maar op vertrouwen dat dit niet gebeurt.

Q Vertrouwen in de overheid?

Bij de Piratenpartij vinden we vertrouwen belangrijk; toch willen wij ook de mogelijkheid tot controle, juist bij de overheid. Wij willen namelijk een transparante overheid, geen transparante burger. We snappen dat het niet de bedoeling is dat er misbruik gemaakt wordt van wetgeving, maar ervaring leert dat politie, justitie en geheime diensten altijd maximaal gebruik zullen maken van de mogelijkheden die ze hebben. *Hiervoor vinden we het belangrijk dat de verwachtingen en verplichtingen van bijvoorbeeld de geheime diensten duidelijk zijn omschreven, zodat hier ook aan getoetst kan worden. Bijvoorbeeld door zowel de TIB als de CTIVD & CIVD. En voor Kamerleden bij het geplande evaluatiemoment.*

Q Evaluatiemoment?

Ja, over twee jaar vindt er een evaluatiemoment plaats rondom het gebruik van Wiv 2017. Wat er na het evaluatiemoment gebeurt, is op dit moment nog onduidelijk. Wat de Piratenpartij betreft is dit onvoldoende, en is het bij wetgeving die zo een grote inbreuk op je persoonlijke levensomgeving kan maken, van belang dat er een terugkerend moment van evaluatie wordt afgesproken.

Q “Veiligheid of privacy”

Het is een valse tegenstelling om te stellen dat je jouw privacy, jouw vrijheid moet opgeven voor veiligheid. Er is niet bewezen dat de veiligheid daadwerkelijk zal vergroten met de nieuwe mogelijkheden van de geheime diensten. Tot nu toe is bij iedere aanslag gebleken dat de daders reeds in beeld waren. Wat de Piratenpartij betreft gaan we de naald in de hooiberg niet vinden door deze hooiberg nog groter te maken. Met gerichte opsporing kun je je middelen veel beter inzetten.

Q “We kunnen de kabel niet aftappen zonder Wiv 2017”

Gericht aftappen was met Wiv 2002 al prima mogelijk en werd ook gedaan. Deze week is er voor het eerst een rapportage gegeven hoe vaak deze mogelijkheid is ingezet door de geheime diensten. In 2017 is dit 3553 keer gebeurd. Wat niet mogelijk is, is het ongericht aftappen van bijvoorbeeld een hele wijk, of straat.

Q “Als je tegen de Wiv 2017 bent, ben je dus voor Wiv 2002!”

Dit is niet het geval. Als je tegen Wiv 2017 stemt tijdens het referendum van 21 maart, ben je tegen de Wet Inlichtingen en veiligheidsdiensten 2017. Je geeft daarmee aan dat je de Wiv 2017 onvoldoende vindt. Je bent niet per se een voorstander van het behoud van Wiv 2002 en daarmee een tegenstander voor een vernieuwende wet. Vrijwel alle partijen die campagne voeren tegen Wiv 2017 geven aan dat ze een betere, nieuwe wet willen.

Q Betere controle CTIVD/CIVD?

De CTIVD heeft ongekende toegang tot onze inlichtingendiensten: ze kunnen en mogen meer dan gebruikelijk toezicht houden op onze geheime diensten. Hun bevindingen en adviezen zijn echter niet bindend. Dit betekent dat een minister het advies van de CTIVD naast zich neer kan leggen. De CTIVD brengt ook verslag uit aan de CIVD (commissie stiekem). De CIVD is echter verplicht tot geheimhouding, waardoor ze vooral informatie enkel ter kennisgeving kunnen aannemen. Wat de Piratenpartij betreft, maakt dit van de CTIVD vooral een tandeloze tijger, en is het van belang dat de CTIVD ook de mogelijkheid krijgt om een operatie te beëindigen. Eventueel kan dan via een rechter gekeken worden of dit terecht of onterecht is gegaan.

Q “Ik heb niets te verbergen!”

Dat is mooi, maar misschien een beetje saai! En andere mensen dan? Daarnaast weet je nu niet wat er over drie jaar verboden is, of over vijf jaar, of tien jaar. Of in een buitenland waarmee wij gegevens uitwisselen. Iets dat nu perfect normaal is, kan over tien jaar zomaar verboden zijn en dan hebben we deze wet ineens wel. Daarnaast: dat jij niets te verbergen hebt, betekent niet dat je arts niets te verbergen heeft, of een journalist die namens jou de controle op onze democratie uitvoert. Het recht op

privacy is ook het recht op vrijheid om vrij je leven te kunnen invullen zoals jij dit wilt én om je eigen volksvertegenwoordigers vrij te kunnen controleren.

Q: En beveiligingslekken?

Met deze wet krijgt onze geheime dienst de bevoegdheid om bij een fabrikant onbekende computer-veiligheidslekken te gebruiken om computersystemen te hacken. Hiervoor zorgen de geheime diensten er (onbedoeld) voor dat al onze computersystemen onveiliger worden. Immers, als beveiligingslekken niet meer gemeld worden bij een fabrikant om hersteld te worden, dan nemen we met elkaar het risico dat uiteindelijk criminelen dezelfde lekken zullen gaan gebruiken.

Q: Wat is dat eigenlijk, die DNA-databank?

Inlichtingendiensten mogen met de Wiv 2017 een DNA databank creëren waarin DNA-gegevens van verdachten en niet-verdachten kunnen worden opgenomen voor een periode van 30 jaar. Inlichtingendiensten zijn ook niet beperkt in waar ze deze gegevens vandaan mogen halen. Dit geeft de overheid het recht een geheime DNA-databank te beheren zonder dat we enig inzicht hebben in welke gegevens er in staan en wat er mee gebeurt.

Q: En het recht op privacy dan?

Het recht op privacy is verankerd in artikel 10 van onze grondwet. Echter beslist artikel 120 van dezelfde grondwet dat onze rechter niet mag toetsen of onze wetten wel of niet tegen de grondwet in gaan. Omdat de Wiv 2017 tegen de grondwet in lijkt te gaan, maar je dat niet aan een rechter kunt voorleggen, zullen eventuele rechtszaken vooral op basis gaan van Europees recht.

Q Wat moet er gebeuren als Wiv 2017 weggestemd is?

Het is duidelijk dat deze wet onvoldoende is: tijdens de internetconsultatieronde voorafgaand aan deze wet waren er 557 reacties met opmerkingen en verbeterpunten voor deze wet. De overheid is verplicht deze consultatie mee te nemen bij het creëren van wetgeving. De Piratenpartij ziet deze opmerkingen niet terugkomen in de huidige wetgeving. Wat ons betreft is een goed uitgangspunt om opnieuw te kijken naar alle informatie die tijdens deze internetconsultatieronde is binnengekomen, om vervolgens een betere Wiv te maken. De Piratenpartij wil in ieder geval de ‘onderzoeksopdrachtgerichte interceptie’ vervangen door ‘gerichte interceptie’, betere kaders en bindende toetsing. Gegevens mogen enkel na eerste eigen analyse worden gedeeld met buitenlandse inlichtingendiensten, en beveiligingsproblemen dienen gemeld te worden aan de fabrikant zodat alle computers veiliger kunnen worden.

Andere vragen? Plaats een reactie en stel ze!

## 2: NGO's and Interest Groups

### Amnesty International: Sleepwet Bedreiging voor Mensenrechten

Sleepwet: 3 redenen om tegen te stemmen

Op 21 maart 2018 wordt tijdens de gemeenteraadsverkiezingen ook een raadgevend referendum gehouden. Nederland stemt dan voor of tegen de nieuwe Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv), ook wel bekend als de Sleepwet. Amnesty heeft grote zorgen over deze wet, omdat die onnodig onze privacy en vrije meningsuiting bedreigt. Ook kunnen onze gegevens in verkeerde handen terechtkomen. We willen een wet die onze veiligheid én onze mensenrechten beschermt. Daarom adviseren wij: stem tegen de Sleepwet op 21 maart. Zo roep je de regering op de wet te verbeteren.

1. Jouw privacy staat op het spel

De regering hoort haar burgers en de democratische rechtstaat te beschermen tegen dreigingen. Daarvoor hebben de Nederlandse inlichtingen- en veiligheidsdiensten voldoende bevoegdheden nodig om die dreigingen te kunnen onderzoeken. Maar met de nieuwe wet mogen de diensten nu met een 'sleepnet' ook communicatie via de kabel stelselmatig en op grote schaal onderscheppen. Dus ook de gegevens van grote groepen mensen die geen bedreiging vormen voor de samenleving.

Daarom zegt Amnesty: gegevens van mensen die geen bedreiging zijn voor de nationale veiligheid zouden niet stelselmatig en op grote schaal verzameld en geanalyseerd moeten kunnen worden.

Als je niets verkeerd hebt gedaan, waarom wordt jouw privacy dan niet gerespecteerd? Dat is een terechte vraag. Durf je 'jihad' nog als zoekterm te gebruiken om jezelf te informeren? Je hebt niet in de hand welke conclusies die diensten trekken uit de gegevens die ze verzamelen. En regeringen wisselen elkaar af. Je weet dus niet wie het straks voor het zeggen krijgt en welke gegevens dan interessant zijn.

2. Jouw gegevens in verkeerde handen?

De wet staat toe dat gegevens ongefilterd gedeeld mogen worden met buitenlandse geheime diensten, dus zonder te weten waar ze precies over gaan. De wet staat zelfs toe dat die gegevens gedeeld mogen worden met landen waar mensen worden onderdrukt. Dat kan grote gevolgen hebben. Zo weten we dat sommige regeringen privéinformatie gebruiken om journalisten of bloggers tegen te werken, activisten te vervolgen, homoseksuelen en lesbiennes te discrimineren en de vrije meningsuiting te onderdrukken.

Ook jouw gegevens mogen niet in verkeerde handen terechtkomen. Wellicht denk je 'ik heb niets te verbergen, dus wat maakt het uit.' Dat klinkt logisch, maar informatie die voor jou onschuldig is, kan voor een regering verdacht materiaal zijn. De Nederlandse toezichthouder heeft wel zicht op welke gegevens gedeeld worden, maar kan niet nagaan waar ze daadwerkelijk voor worden gebruikt.

Daarom zegt Amnesty: deel nooit ongefilterde gegevens met buitenlandse geheime diensten.

Stel: Er is een onderzoek naar mensen die in Syrië de strijd van Islamitische Staat steunden en mogelijk willen terugkeren naar ons land. De communicatie vanuit Syrië met een bepaalde stad in Nederland wordt hiervoor onderzocht. De Nederlandse dienst vraagt aan de Turkse geheime dienst informatie over mensen die via Turkije reizen. Die wil de Turkse dienst wel geven, mits ze daar de door Nederland onderschepte gegevens voor terug krijgen. Het kan dus gebeuren dat jouw kritische berichten over Turkije of over president Erdoğan worden gedeeld met Turkije. Voor de Nederlandse inlichtingendienst wellicht niet zo interessant, maar voor de Turkse geheime dienst mogelijk wel. Vooral als je een Turkse achtergrond hebt, zou dat gevolgen kunnen hebben voor jouw volgende bezoek aan Turkije.

3. *De toezichthouder moet achteraf bindend kunnen oordelen*

In een vrije, democratische samenleving is het belangrijk dat iedereen zich aan de spelregels houdt. In een vrije maatschappij controleert de samenleving de overheid. Omdat de inlichtingen- en veiligheidsdiensten in het geheim werken, is controle echter lastig. Daarom is het van groot belang dat er een externe, onafhankelijke, onpartijdige toezichthouder is die bindend kan oordelen of de geheime diensten hun activiteiten rechtmatig hebben uitgevoerd. Dat garandeert dat er wordt getoetst op machtsmisbruik.

Deze externe toezichthouder bestaat al: de CTIVD, de Commissie van Toezicht voor de inlichtingen- en veiligheidsdiensten. Als een onderzoek naar het handelen van de geheime diensten is afgerond, deelt de CTIVD de bevindingen met de minister en met de Tweede Kamer. Maar deze bevindingen zijn niet bindend: de minister kan ze naast zich neerleggen. *Dus als de CTIVD constateert dat de geheime diensten hun activiteiten onrechtmatig uitvoeren, dan kan deze de diensten niet bevelen de activiteiten te stoppen en de gegevens die onrechtmatig verzameld zijn te vernietigen.*

Daarom zegt Amnesty: zorg voor een toezichthouder die achteraf bindend over de uitvoering van de activiteiten van de geheime diensten kan oordelen. Lees hier over toezicht vooraf.

**Extra: (FAQ)**

De Wet op de inlichtingen- en veiligheidsdiensten, ook Sleepwet genoemd, bedreigt onnodig onze privacy en vrije meningsuiting. De regering hoort haar burgers en de democratische rechtstaat te beschermen tegen dreigingen. Daarvoor hebben de Nederlandse inlichtingen- en veiligheidsdiensten voldoende bevoegdheden nodig om die dreigingen te kunnen onderzoeken. De maatregelen die getroffen worden – de wetten die gemaakt worden om de democratische rechtstaat en haar burgers te beschermen tegen aanslagen en andere dreigingen – moeten niet de rechten en vrijheden die diezelfde democratische rechtstaat biedt, ondermijnen.

Met de nieuwe wet mogen de diensten met een ‘sleepnet’ straks ook communicatie via de kabel stelselmatig en op grote schaal onderscheppen. Dus ook de gegevens van grote groepen mensen die geen bedreiging vormen voor de samenleving. Hoe vrij voel jij je dan nog om je mening te delen via e-mail of WhatsApp, of je medische gegevens?

Als je niets verkeerd hebt gedaan, waarom wordt jouw privacy dan niet gerespecteerd? Dat is een terechte vraag. Durf je ‘jihad’ nog als zoekterm te gebruiken om jezelf te informeren? Meld je wantoestanden bij de overheid nog aan een journalist als je weet dat het gesprek via het sleepnet kan worden onderschept? Je hebt niet in de hand welke conclusies die diensten trekken uit de gegevens die ze verzamelen. En regeringen wisselen elkaar af. Je weet dus niet wie het straks voor het zeggen krijgt en welke gegevens dan interessant zijn.

De toezegging van de minister in het regeerakkoord dat ‘van het willekeurig en massaal verzamelen van gegevens van burgers in Nederland en het buitenland geen sprake kan, mag en zal zijn’ is betekenisloos. In een rechtstaat is legitiem overheidsoptreden immers nooit willekeurig. De overheid schrijft geen willekeurige boetes uit en legt geen willekeurige belastingen op. En het massaal verzamelen van gegevens is juist wat beoogd wordt met de sleepnetbevoegdheid. Dat blijkt uit de reactie van het vorige kabinet op een amendement van D66.

Volgens zowel de huidige als de nieuwe wet mogen de inlichtingen- en veiligheidsdiensten gericht kabel- en niet-kabelgebonden communicatie onderscheppen. Gericht betekent hier dat het moet gaan om communicatie van een specifiek persoon, organisatie of technisch kenmerk (zoals een telefoonnummer). Ongericht onderscheppen mag nu ook al, maar alleen niet-kabelgebonden communicatie, zoals satelliet- en radioverkeer. De nieuwe wet noemt dit laatste nu onderzoeksopdrachtgerichte interceptie, waarbij straks ook communicatie via internet onderschept mag worden.

Gegevens die niet relevant zijn voor het onderzoek waarvoor ze verzameld zijn óf die in het kader van een andere onderzoeksopdracht zijn verzameld, moeten zo snel mogelijk vernietigd worden. Gegevens die niet op relevantie zijn onderzocht mogen drie jaar bewaard worden. Deze gegevens mogen gebruikt worden in metadata-analyses en mogen volgens de wet uitgewisseld worden met buitenlandse diensten.

**Ik heb niets te verbergen**

Het gaat er niet om of je wel of niet iets te verbergen hebt. Het ‘ik-heb-niets-te-verbergen’-argument zet privacy neer als een ondeugd in plaats van een vrijheid. Het verlangen naar privacy is geen indicatie van crimineel gedrag. Privacy is van groot belang voor autonomie en menselijke waardigheid. Bovendien is privacy een belangrijke fundering voor andere mensenrechten.

Privacy stelt je in staat om grenzen te stellen en jezelf te beschermen tegen tegen ongewilde inmenging in je leven. Zo heb je de ruimte om te onderzoeken en bepalen wie je bent en hoe je de wereld om je heen tegemoet wil treden. Privacy helpt je om grenzen te stellen aan wie je in je huis laat, wie aan je spullen mag komen, met wie je lichamelijk contact hebt, maar ook aan wie toegang heeft tot jouw communicatie en informatie.

**Free Press Unlimited**

Een groep Amsterdamse studenten heeft een raadgevend referendum aangevraagd over de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten. De studenten vinden dat er een publiek debat zou moeten plaatsvinden over de wet “vanwege de grote gevolgen voor de vrijheid van burgers”. Met deze nieuwe wet kunnen de geheime diensten namelijk op grote schaal onze communicatie tappen, zelfs al vormen we geen bedreiging.

Free Press Unlimited heeft voor en achter de schermen campagne gevoerd tegen de invoering van het zogenaamde sleepnet dat in de wet is opgenomen. Wanneer de wet in werking treedt – naar alle waarschijnlijkheid op 1 januari 2018 – hebben de Inlichtingen- en Veiligheidsdiensten de mogelijkheid om massaal data en communicatie te verzamelen van het internet. Een verregaande schending van de privacy van onschuldige burgers en een grote bedreiging voor de persvrijheid in Nederland.

Sleepnet desastreus voor de journalistiek

Het sleepnet kan op grote schaal communicatie onderscheppen waardoor het voor journalisten onmogelijk wordt om hun bronnen bronbescherming te garanderen. Je weet immers niet of jouw communicatie met een journalist in het sleepnet terecht komt. Wanneer bronnen terughoudend worden in het delen van informatie met journalisten omdat ze bang zijn dat de diensten meelezen of -luisteren kunnen journalisten hun functie als waakhond van onze democratie niet meer vervullen. Belangrijke verhalen met maatschappelijke relevantie dreigen dan niet naar buiten komen. Denk bijvoorbeeld aan het Watergate-schandaal of de Panama Papers.

De privacy van onschuldige burgers wordt onnodig aangetast. Sociologisch onderzoek toont aan dat wanneer mensen het gevoel hebben dat ze gevolgd worden ze hun gedrag aanpassen en zich sociaal wenselijk gaan gedragen. Als de Inlichtingen- en Veiligheidsdiensten misschien wel meelezen, zie je er misschien toch maar van af om gevoelige informatie te delen met een journalist.

De effectiviteit van een sleepnet voor de bevordering van veiligheid is niet aangetoond. Ook in het Verenigd Koninkrijk, Frankrijk en Duitsland is massasurveillance toegestaan, maar dat heeft geen aanslagen kunnen tegenhouden. Steeds blijkt dat informatie over daders al in het sleepnet zat, maar door de grote hoeveelheid data die wordt verzameld, zien de diensten door de bomen het bos niet meer.

Het referendum

Om het referendum door te laten gaan, moeten de initiatiefnemers moeten voor 16 oktober 2017 minimaal 300.000 handtekeningen verzamelen. In Nederland hebben we nog nooit op grote schaal het debat gevoerd over de vraag wat burgers willen dat de overheid van hen weet. Free Press Unlimited steunt dan ook het initiatief van de studenten.

**Nieuwe wet op de inlichtingen- en veiligheidsdiensten: onvoldoende balans tussen veiligheid en privacy**

**7 februari 2017 - Laatste update 22 december 2017**

Het voorstel voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv) heeft grote gevolgen voor de privacy van iedereen in Nederland. Ook de vrijheid van meningsuiting en de persvrijheid kunnen in gevaar komen. Een wetsvoorstel dat zulke gevolgen heeft op mensenrechten mag niet worden ingevoerd zonder goede wettelijke bescherming tegen misbruik en stevig toezicht. En hierin schiet het wetsvoorstel te kort vindt het College.

Nieuwe wet op de inlichtingen- en veiligheidsdiensten: onvoldoende balans tussen veiligheid en privacy

Woensdag 8 februari debatteert de Tweede Kamer over dit wetsvoorstel, waarin de bevoegdheden van de veiligheidsdiensten flink worden uitgebreid. Zo maakt het wetsvoorstel het voor de veiligheidsdiensten mogelijk om op veel grotere schaal dan nu alle vormen van telecommunicatie te onderscheppen. Denk hierbij aan het aftappen van telefoon- en e-mailverkeer of aan het opvangen van berichten op social media. De diensten krijgen ook meer mogelijkheden om computers binnen te dringen.

In 2015 heeft het College al een kritisch advies gegeven over een eerdere versie van het wetvoorstel. Sindsdien is het wetsvoorstel op een aantal punten gewijzigd. De huidige tekst van het wetsvoorstel zorgt al voor een betere bescherming van de mensenrechten. En de toelichting die de regering heeft gegeven naar aanleiding van vragen uit de Tweede Kamer zorgt voor extra duidelijkheid over de

omvang van de nieuwe afluisterbevoegdheden. Daar is het College blij mee. Toch komt het College tot de conclusie dat het toezicht en de bescherming nog steeds niet stevig genoeg geregeld zijn. Er is nog steeds geen goede balans tussen privacy en veiligheid. En daar ligt de uitdaging in dit wetsvoorstel.

Ter voorbereiding op het debat zet het College in een brief aan de Tweede Kamer de nog bestaande knelpunten en onduidelijkheden op een rij. *Het is vooral belangrijk dat de positie van de onafhankelijke toezichthouder (de CTIVD) wordt versterk*t. Deze instantie moet de bevoegdheden krijgen om effectief toezicht uit te voeren gedurende de daadwerkelijke uitvoering van de operaties door de diensten. En de wet moet op een paar plaatsen aangescherpt om de CTIVD heldere normen voor dat toezicht te bieden.

**Bits of Freedom – eenbeterewet.nl – Dit zijn de 5 verbeterpunten**

Er kan nu al gericht communicatie op internet (de kabel) en ongericht communicatie uit de lucht (bijvoorbeeld militair communicatieverkeer) worden onderschept door de geheime diensten. Met de nieuwe wet kan er straks massaal en stelselmatig communicatie opgevist worden met een sleepnet. Bijvoorbeeld alle communicatie die langs de wifi-hotspots van een grote provider in een stad komt, mogen ze opvissen. Onschuldige burgers horen niet in het vizier van de geheime diensten. Wij vinden dat deze bevoegdheid (art. 48 en verder) in zijn huidige vorm uit de wet moet.

Internationale samenwerking tussen geheime diensten is belangrijk, maar mag niet zover gaan dat gegevens over onschuldige burgers in handen komen van buitenlandse geheime diensten. Dit dreigt nu wel te gebeuren met de nieuwe wet.

De gegevens die de geheime diensten binnen halen (o.a. via het sleepnet) kunnen worden gedeeld met buitenlandse diensten, zonder deze gegevens eerst te analyseren. Door gegevens uit te wisselen die de geheime diensten niet eerst zelf geanalyseerd hebben, weten ze niet waar de gegevens precies over gaan. Ze kunnen dus onvoldoende een inschatting maken van de gevolgen van het delen van deze gegevens. Stel je voor dat jouw bezoek aan websites die kritisch berichten over een buitenlandse politieke leider worden gedeeld met dat desbetreffende land? Dat is onacceptabel.

De mogelijkheid om ongeëvalueerde gegevens te verstrekken aan het buitenland moet uit de wet worden geschrapt (zie art. 64 en 88).

Volgens de nieuwe wet kan elke organisatie of persoon samenwerken met de geheime diensten door hen toegang te geven tot hun databases. Denk dan aan toegang tot de database van bijvoorbeeld onderwijsinstellingen, banken of je persoonlijke documenten bij een cloudprovider. Het zomaar weggeven van die gegevens kan een hele grote privacy-inbreuk opleveren. Men hoeft niet mee te werken met de geheime diensten, maar het is de vraag of men dit durft te weigeren.

Bits of Freedom vindt dat de geheime diensten niet die druk bij een persoon or organisatie neer moet leggen. De wet moet hierop aangepast worden. *Er zal hier meer toezicht op moeten komen, zoals toestemming van de minister en de toetsingscommissie.*

Dit is de benaming voor het gebruik maken van onbekende zwakke plekken in software. Die noemen we onbekend, omdat de maker van de software ze nog niet kent. De geheime diensten gebruiken deze zwakke plekken om apparaten te hacken. Het probleem hierbij is dat iedereen die gebruik maakt van die software die zwakke plek dan heeft, de maker van de software niet op de hoogte is, het niet kan oplossen en daarmee ook andere overheden of criminelen hun gang kunnen gaan. Want het zijn niet alleen de geheime diensten die hier naar speuren. Door deze

zwakke plekken niet te melden bij de maker, maken de geheime diensten ons niet veiliger maar juist onveiliger. Het is namelijk een illusie om te denken dat alleen de Nederlandse geheime diensten die kwetsbaarheden vinden.

De geheime diensten moeten onbekende zwakke plekken daarom altijd op verantwoorde wijze melden bij de maker van de software. Op basis van de nieuwe wet hoeft dat niet. Dit moet aangepast worden in de wet.

Er is een onafhankelijke toezichthouder die toezicht houdt op de geheime diensten, de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (de CTIVD). Die toetst achteraf of de geheime diensten hun werk wel volgens de wet doen en kunnen oordelen dat de geheime diensten zich niet aan de regels houden. De minister kan dit naast zich neerleggen, het oordeel van de CTIVD is namelijk niet bindend.

*De toezichthouder moet meer tanden krijgen, als de diensten in overtreding zijn moet dit direct door de CTIVD gestopt kunnen worden. De wet moet worden aangepast zodat de oordelen van de toezichthouder bindend zijn.*

**Privacy First: Sleepnet – ABC**

**Hieronder treft u de voornaamste bezwaren van Privacy First aan tegen de nieuwe Wet op de inlichtingen en veiligheidsdiensten (Wiv2017 of 'Sleepwet'), in alfabetische volgorde:**

A. Aftappen

Door de bevoegdheid van 'onderzoeksopdrachtgerichte interceptie' - in de volksmond ook wel sleepnet genoemd - wordt het mogelijk voor de inlichtingen- en veiligheidsdiensten (geheime diensten) om het internetverkeer van grote groepen mensen tegelijk af te tappen. Zo kan er een tap worden geplaatst op een bepaalde gemeente, een wijk, buurt of straat, indien daar een ‘target’ van de geheime dienst woont. Daarbij wordt de communicatie van onschuldige burgers verzameld door middel van een digitaal sleepnet. Privacy First is van mening dat de gegevens van onschuldige burgers niet thuis horen bij de inlichtingendiensten. Bovendien neemt de effectiviteit van de inlichtingendiensten af door de te grote hoeveelheid aan vergaarde data.

B. Buitenland

Gegevens die vergaard zijn met het sleepnet mogen onder de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Sleepwet) ongeëvalueerd met het buitenland gedeeld worden. Dit betekent dat de Nederlandse inlichtingendiensten ongeziene en ongeselecteerde gegevens (van onschuldige burgers) met buitenlandse geheime diensten kunnen delen. Op het gebruik van deze gegevens is vervolgens geen toezicht meer te houden door de Nederlandse diensten.

Bewaartermijnen

Ongeëvalueerde gegevens die door middel van het sleepnet zijn verzameld, mogen drie jaar worden bewaard. Deze ongeëvalueerde gegevens mogen ook ongezien met het buitenland worden gedeeld.

Gegevens die de inlichtingen- en veiligheidsdiensten relevant hebben bevonden, mogen bewaard worden zolang deze nog relevant zijn.

C. CTIVD

*Het oordeel van de onafhankelijke toezichthouder CTIVD (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten) die achteraf toetst of de bevoegdheden rechtmatig zijn ingezet, is niet bindend. De minister kan de bevindingen en aanbevelingen naast zich neer leggen en eventueel doorgaan met het onrechtmatig inzetten van bevoegdheden.*

Chilling effect

De nieuwe wet kan er voor zorgen dat mensen zich (onbewust) anders gaan gedragen dan ze zich zouden gedragen in een vrije omgeving. Dit kan een negatief effect hebben op de uitoefening van andere grondrechten dan het recht op privacy, zoals de vrijheid van meningsuiting of de vrijheid van vereniging, vergadering en demonstratie.

D. Databanken

De nieuwe wet maakt directe, automatische toegang tot databanken in de gehele private én publieke sector mogelijk. Hiermee kunnen de inlichtingendiensten rechtstreeks toegang krijgen tot allerlei gevoelige databanken bij bedrijven, overheidsinstanties en andere organisaties, hetzij middels informanten of agenten (infiltranten) bij die organisaties, hetzij middels geheime overeenkomsten.

Decryptiebevel

Door de nieuwe wet dienen versleutelde data bij bedrijven, overheden of particulieren (bijvoorbeeld communicatiedata) op verzoek van de geheime dienst ontsleuteld te worden. Weigering om aan een decryptiebevel te voldoen wordt bestraft met 2 jaar hechtenis.

DNA-databank

Met de invoering van de wet krijgen de inlichtingen- en veiligheidsdiensten een eigen DNA-databank. Ze mogen het DNA verzamelen van zogenoemde ‘targets’ (doelwitten) en ‘non-targets’ (onschuldige burgers). Om dit DNA te verzamelen mag de inlichtingen- en veiligheidsdienst zich o.a. toegang verschaffen tot een besloten plaats, bijvoorbeeld een kantoor of woning. De Groene Amsterdammer heeft een zeer uitgebreid stuk geschreven over de “DNA Verzameldienst”, dit is hier te lezen.

E. Europees Verdrag voor de Rechten van de Mens (EVRM)

Het recht op privacy is een mensenrecht: dit recht wordt beschermd door artikel 8 van het EVRM. Privacy First is van mening dat de nieuwe Sleepwet het recht op privacy schendt. Privacy First heeft dan ook een (concept)dagvaarding klaarliggen om de Staat voor de rechter te slepen zodra de Sleepwet in werking treedt. De rechter kan de Sleepwet dan toetsen en (deels) buiten werking stellen wegens schending van art. 8 EVRM.

F. Fake news door Nederlandse overheid

Volgens onze minister van Binnenlandse Zaken Ollongren is het niet noodzakelijk dat de overheid op haar website rijksoverheid.nl neutrale informatie plaatst over het Sleepwet-referendum. Hierdoor wordt er door de overheid geen objectieve informatie verstrekt aan de kiezers.

G. Geautomatiseerde werken

Zoals onder 'hackbevoegdheid' en "Internet of Things' uitgelegd, zullen door de Sleepwet alle apparaten gehackt mogen worden door de geheime diensten.

H. Hackbevoegdheid

Onder de nieuwe wet krijgen de inlichtingendiensten de mogelijkheid om een target te hacken via onschuldige derden. Dit houdt in dat de inlichtingendienst door het hacken van een derde (tante, zus, vriend, vriendin, echtgenoot, opa, collega, buurman, werk, overheid, bedrijf etc.) toegang krijgt tot informatie over het doelwit van de dienst. Dit betekent dat de apparaten van onschuldige burgers gehackt kunnen worden door de diensten. Deze burgers zullen hiervan nooit op de hoogte raken (er geldt hiervoor geen notificatieplicht).

I. Ik heb niks te verbergen

Iedereen heeft recht op een privéleven. De gegevens van onschuldige burgers horen daarom niet thuis bij de inlichtingen- en veiligheidsdiensten. Deze gegevens met onder andere medische informatie, persoonlijke gesprekken, privé emails, zakelijke emails, nieuwsberichten, hobbies, interesses en internet-zoekresultaten dienen daarom goed te worden beschermd. Daarnaast heeft u misschien 'niets' te verbergen, maar andere burgers zoals medische professionals, advocaten, activisten, klokkenluiders en journalisten wel.

Internet of Things

Steeds meer apparaten zijn op het internet aangesloten. Al deze apparaten kunnen onder de Sleepwet afgeluisterd of gehackt worden. Te denken valt aan een auto, camera, microfoon, printer maar eventueel ook zelfs een pacemaker. De Sleepwet sluit deze mogelijkheid immers niet uit.

J. Journalisten

De communicatie van journalisten kan met de nieuwe wet worden onderschept, door onder andere de inzet van het sleepnet. De geheime diensten kunnen dan van deze informatie kennis nemen. Dit vormt een bedreiging voor de persvrijheid en het journalistieke brongeheim. Pas achteraf zullen de diensten de informatie die niet noodzakelijk is voor het onderzoek zo snel mogelijk verwijderen.

K. Kabelgebonden interceptie

Onterecht wordt er gespeculeerd dat de inlichtingen- en veiligheidsdiensten momenteel niet op de kabel mogen aftappen en enkel via de ether. De inlichtingen- en veiligheidsdiensten mogen onder de huidige wet een tap plaatsen op de kabel, wanneer dit gericht is op bijvoorbeeld één individu. Met de nieuwe wet krijgen de inlichtingen- en veiligheidsdiensten de bevoegdheid om ongericht en grootschalig de kabel af te tappen (sleepnet).

L. Lubach

Arjen Lubach heeft in zijn uitzendingen van Zondag met Lubach drie items gemaakt over de Sleepwet en waarom het goed is om hier kritisch op te zijn. De filmpjes zijn hier te bekijken: Sleepwet 1, Sleepwet 2 en Sleepwet 3.

M. Mensenrechten

Privacy is een mensenrecht. Dit recht op bescherming van de persoonlijke levenssfeer geldt voor iedereen en wordt door talloze internationale en Europese verdragen gewaarborgd. Door de Sleepwet wordt dit recht massaal geschonden, aangezien de data van grote groepen onschuldige burgers door deze wet zullen worden verzameld, opgeslagen en internationaal uitgewisseld.

Medisch beroepsgeheim

Door de nieuwe wet kan de medische privacy van patiënten en het medisch beroepsgeheim van artsen niet gegarandeerd worden: de geheime diensten mogen bij iedereen, ook bij artsen en ziekenhuizen, relevante gegevens opvragen en toegang tot hun data-systeem (Elektronisch Patiëntendossier) vragen of dergelijke systemen hacken. Dit kan bovendien leiden tot zorgmijdend gedrag bij patiënten en daarmee tot een bedreiging van de volksgezondheid.

N. Notificatieplicht

De notificatieplicht in de nieuwe wet schiet tekort. Vijf jaar na de inzet van een bevoegdheid onder de Sleepwet dient de betreffende persoon hierover in principe te worden geïnformeerd. Dit geldt echter slechts voor enkele van de nieuwe bevoegdheden. Privacy First is van mening dat de notificatieplicht moet gelden voor de inzet van álle bevoegdheden.

O. Onschuldpresumptie

Met de invoering van de nieuwe wet wordt het onschuldbeginsel omgedraaid. Door het sleepnet wordt potentieel elke burger 'verdacht', zonder concrete aanleiding om die burger te volgen. Daarnaast wordt de kans op false positives (onterechte verdenkingen) bij massale datavergaring erg groot.

P. Privacy

De privacy van onschuldige burgers wordt door de inzet van de Sleepwet geschonden. Zie hiervoor alle andere argumenten.

Q. Queeste naar data

Bij de overheid is een hongerlust naar data ontstaan. Waar landen om ons heen teruggaan naar een gerichte aanpak, gaat Nederland voor Big Data. Hierdoor wordt er steeds meer hooi verzameld en zal de speld steeds moeilijker te vinden zijn. Meer data zorgt niet meteen voor meer veiligheid.

R. Rechter

Een gerechtelijke toets vooraf aan de inzet van de bevoegdheden ontbreekt veelal. Zoals onder “TIB’ uitgelegd, mist de nieuwe toetsingscommissie de onderzoeksbevoegdheden voor effectief en onafhankelijk toezicht.

S. Sleepnet

Zie ‘Aftappen’

Strafbare feiten

Geheime agenten zijn zowel onder de huidige als de nieuwe wet bevoegd om strafbare feiten te plegen. De precieze reikwijdte van deze bevoegdheid is tot op heden echter onbekend. Onder de huidige wet kon deze bevoegdheid nader worden gereguleerd middels een (nooit ingevoerde) Algemene Maatregel van Bestuur (AMvB). De Commissie Dessens adviseerde enkele jaren geleden om die AMvB alsnog in te voeren. In de nieuwe Sleepwet is de grondslag voor deze AMvB echter geschrapt, waardoor sprake blijft van een juridisch vacuüm.

T. TIB

Onafhankelijk toezicht op alle fasen van de inzet van bevoegdheden door de diensten (voor, tijdens en achteraf) is onvoldoende gewaarborgd. Aangezien de inlichtingendiensten heimelijk opereren, kunnen burgers waartegen de bevoegdheden worden ingezet niet zelf bezwaar maken. Hiervoor dient de inzet van bevoegdheden onafhankelijk te worden getoetst. De nieuwe Toetsingscommissie Inzet Bevoegdheden (TIB) toetst vooraf slechts of de minister terecht toestemming heeft gegeven voor de inzet van een relatief zware ('bijzondere') bevoegdheid onder de nieuwe wet. Deze toetsing is met minder waarborgen omkleed dan toetsing door de rechter. Daarnaast heeft de TIB geen eigen onderzoeksbevoegdheden en is compleet afhankelijk van de informatie die hen wordt gegeven. Verscheidene instanties, zoals de Autoriteit Persoonsgegevens, hebben gewaarschuwd dat moet worden voorkomen dat de TIB een ‘stempelmachine’ zal zijn.

T. Terreurschwalbe

Door voorstanders van de Sleepwet zal vaak het argument aangehaald worden dat deze wet aanslagen zal voorkomen, Zondag met Lubach liet dat zien. In andere landen is echter al gebleken dat gericht werken veel effectiever is. De tegenstanders van de Sleepwet zijn het er over eens dat de huidige wet aan vernieuwing toe is, maar eisen ook dat de wet op cruciale punten wordt aangepast en verbeterd.

U. Uitwisseling van gegevens

Zoals onder ‘Buitenland’ omschreven, kunnen de gegevens van onschuldige burgers en journalisten die worden verzameld door de inzet van het sleepnet, ongezien gedeeld worden met buitenlandse geheime diensten.

V. Veiligheid

Onterecht worden privacy en veiligheid tegenover elkaar gezet. In een vrije democratische samenleving gaan privacy en veiligheid hand in hand. Er kan een goede Wet op de inlichtingen- en

veiligheidsdiensten worden opgesteld met goede privacywaarborgen, waarbij de informatie van onschuldige burgers niet bij de inlichtingendiensten terecht komt.

W. Waarborgen

De wet geeft te grote bevoegdheden aan de inlichtingen- en veiligheidsdiensten en te weinig privacywaarborgen voor burgers. Na het referendum dient de wet terug naar de tekentafel te gaan, van fatsoenlijke waarborgen te worden voorzien en op de inzet van bevoegdheden te worden herzien.

Z. Zero-days

De inlichtingen- en veiligheidsdiensten hebben de bevoegdheid om gebruik te maken van onbekende zwakke plekken (zogenaamde zero-days) in software. Voor de inlichtingen- en veiligheidsdiensten zijn deze kwetsbaarheden dan bekend, maar voor de makers of fabrikanten van de software niet. De inlichtingen- en veiligheidsdiensten hoeven deze kwetsbaarheid niet te melden aan de fabrikant van de software. Hierdoor kunnen eventuele kwaadwillenden (langdurig) misbruik maken van deze kwetsbaarheden. Ook ontstaat hierdoor een zwarte markt voor handel in dergelijke kwetsbaarheden en datalekken.

**Transperancy International Nederland:**

Sleepwet tast bronbescherming aan en schrikt potentiële klokkenluiders af

Lotte Rooijendijk10 oktober 2017Algemeen, Feature, Klokkenluiders, Nationaal, Nieuws, Opinie, Wetgeving
Amsterdam, 10 oktober 2017 – (opiniestuk Lotte Rooijendijk) – Op 11 juli 2017 ging de Eerste Kamer akkoord met een nieuwe Wet op inlichtingen- en veiligheidsdiensten (Wiv), ook wel de sleepwet genoemd. Deze wet staat inlichtingendiensten toe om op grote schaal meerdere soorten gegevens te onderscheppen. Ook bevestigde minister Plasterk dat de nieuwe wet toestaat dat anonieme bronnen van journalisten achterhaald worden. Het was al niet goed gesteld met de bescherming van bronnen in Nederland en het Europees Hof voor de Rechten van de Mens heeft ons land dan ook meermaals veroordeeld voor haar gebrekkige bronbescherming. Desalniettemin werd een amendement (ingediend door D66) om journalistieke bronbescherming te verzekeren in de Wiv, verworpen door de Tweede Kamer. De gebrekkige bronbescherming leidt ertoe dat nog maar weinig mensen de cruciale stap durven te zetten hun informatie te delen. Nu de Eerste Kamer ingestemd heeft, zal de omstreden wet per 1 januari 2018 in werking treden. Dat is niet het einde van de strijd: er wordt geprobeerd een referendum over de sleepwet af te dwingen, zodat de Nederlandse bevolking zich hierover uit kan spreken.

De vernieuwde Wet op de inlichtingen- en veiligheidsdiensten, ook wel sleepwet of aftapwet, geeft een uitbreiding van de middelen die de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) mogen inzetten.

De grootste veranderingen zijn:

• Er mag een zogenaamd “sleepnet” worden ingezet om massaal online communicatie af te luisteren, ook van niet-verdachte burgers. Zo mag uw hele wijk afgeluisterd worden wanneer daar één verdacht persoon woont.
• Alle geautomatiseerde apparaten mogen worden gehackt. Daarbij kunt u denken aan uw eigen telefoon of computer.
• Er mag een DNA-databank aangelegd worden waar iedereen, dus ook u, in terecht kan komen.

• Verzamelde data mag met buitenlandse inlichtingendiensten gedeeld worden, ook zonder dat deze eerst geanalyseerd is.

Instanties als de Raad van State, de Wetenschappelijke Raad voor het Regeringsbeleid, de Nederlandse Vereniging van Journalisten, verscheidene wetenschappers en NGOs, waaronder Transparency International Nederland, hebben hun zorgen geuit over deze wet.

Sleepwet zet aan tot zelfcensuur en maakt bronbescherming onmogelijk

De Wiv vervangt een versie van de wet die in 2002 voor het laatst is aangepast. De nieuwe wet geeft de inlichtingendiensten AIVD en MIVD meer bevoegdheden om communicatie grootschalig af te tappen, zelfs als we geen bedreiging vormen. De wetenschap dat deze diensten meekijken, kan leiden tot zelfcensuur en beperkt de vrijheid voor afwijkende opvattingen die juist zo essentieel zijn in een democratische rechtsstaat.
De nieuwe sleepwet voorziet wel in controle op het aftappen, maar niet in het vooraf bepalen van de afzender. Hierdoor is de zogenaamde bijvangst onvermijdelijk. Gegevens die als bijvangst met het sleepnet naar binnen zijn gehaald, kunnen vertrouwelijke informatie bevatten, zoals bijvoorbeeld gesprekken tussen arts en patiënt, advocaat en cliënt of journalist en bron. Bij vertrouwelijke advocaat-cliëntgesprekken belooft minister Plasterk dat de diensten die onbeluisterd weg zullen gooien. Echter, voor vertrouwelijke communicatie tussen een journalist en haar bron geldt geen vernietigingsplicht, waardoor de identiteit van de bron bekend kan worden bij de autoriteiten.

## Verschoningsrecht journalisten niet serieus genomen in Nederland

De Nederlandse wet biedt overigens ook zonder deze sleepwet nog geen goede bescherming voor journalistieke bronnen. Hoewel journalisten bescherming genieten onder het Europees Verdrag van de Rechten van de Mens (EVRM), hebben de Nederlandse inlichtingen- en veiligheidsdiensten daar meermaals mee in strijd gehandeld. Zo veroordeelde Europese Hof voor de Rechten van de Mens Nederland tot drie keer toe voor schendingen van het recht op journalistieke bronbescherming. In 2015 bijvoorbeeld, toen de Hoge Raad oordeelde dat het afluisteren van een Telegraaf-journaliste ‘niet-proportioneel’ was, maar besloot de schending van bronbescherming verder niet te sanctioneren. Wanneer het aan de laars lappen van journalistieke bronbescherming niet wordt gesanctioneerd, is dat een vrijbrief voor de overheid journalisten af te luisteren om zo hun bronnen te kunnen achterhalen.

Hoewel organisaties zoals de Nederlandse Vereniging van Journalisten al jaren pleiten voor bronbescherming, is er pas in mei vorig jaar een wetsvoorstel aanhangig gemaakt die deze bronbescherming beoogt te verankeren in de wet. Het wetsvoorstel Bronbescherming in Strafzaken leidt tot de invoering van een nieuwe bepaling in het Wetboek van Strafvordering, waarmee er een beperkt verschoningsrecht ontstaat voor journalisten en publicisten. De afronding van dat wetsvoorstel laat al lange tijd op zich wachten.

## Bronnen zijn van onschatbare waarde

Voor de journalistiek zijn bronnen van onschatbare waarde, in het bijzonder ook melders die ernstige misstanden onthullen door als insider te kiezen voor het openbaren van (soms vertrouwelijke) informatie via de pers. Een voorbeeld is de grootschalige belastingontwijking die aan het licht is gebracht door LuxLeaks en meer recentelijk de Panama Papers. Indien de bron bekend wordt, kan deze zware repercussies zoals ontslag, vernedering en juridische procedures verwachten. Journalisten die misstanden in de openbaarheid brengen, moeten daarom hun bronnen effectief kunnen beschermen.

Bij gebrek aan goede bescherming treedt een zogeheten chilling effect op. Dit leidt ertoe dat nog maar weinig mensen de cruciale stap durven te zetten zich uit te spreken tegen misstanden door hun

informatie te delen met journalisten. De maatschappelijke rol van de journalist als “waakhond van de samenleving”, die handelt in het belang van de informatievoorziening en het openbare debat in de democratie, wordt hiermee uitgehold. Daarom acht Transparency International Nederland het van groot belang dat het recht op journalistieke bronbescherming ook rechtstreeks in de Nederlandse wetgeving verankerd wordt. Als intern op de werkvloer of extern melden bij het Huis voor Klokkenluiders of andere bevoegde autoriteiten geen optie (meer) is, moeten journalisten vertrouwelijk toegankelijk zijn voor diegenen die informatie hebben over machtsmisbruik, belangenverstrengeling en andere maatschappelijke misstanden.

Door een gebrek aan goede bescherming van bronnen zullen potentiële melders van misstanden minder snel bereid zijn gevoelige informatie te delen. Dit schaadt de nieuwsvoorziening. En als een goede nieuwsvoorziening ontbreekt, hapert de democratie.

**Weblogs:**

**GeenStijl**

**Nederlanders zijn Sleepwetschapen. Allemaal**

Het is bizar dat een Sleepwet kon worden ontworpen, het is beangstigend dat een politieke meerderheid hem wilde aannemen en het is dood- en doodeng dat het miljoenen burgers geen fuck boeit dat het gebeurt.

*(Ollongren als een Medusa met camera’s)*

Ja, het is best OK als de overheid diensten heeft die verdachten, burgers en buitenlui kan onderzoeken, op basis van tips, vermoedens of bestaande feiten, om te weten wat hun motieven en doelen zijn. Maar nee, het is niet OK als de overheid daarvoor systemen bouwt waarmee met een druk op de knop alle data, van alle burgers kan worden opgevist in een sleepnet.

Om je huis binnen te mogen, heeft de politie een redelijke verdenking en een huiszoekingsbevel van een (hulp-) officier van justitie nodig. Om je internetkabels te mogen tappen is er in theorie ook een redelijke verdenking en toestemming nodig. Maar aangezien niemand de ‘deur’ open hoeft te doen als diensten digitaal willen inbreken, wie garandeert ons dan dat er geen misbruik van gemaakt wordt, dat

er altijd oprechte bedoelingen zijn, dat er uit gemakzucht, tijdswinst of gewoon omdat het kan geen misbruik wordt gemaakt van die mogelijkheden?

Taptechnieken om je ex te stalken

Wie zegt dat hier alles zuiver gebeurt? Wie zegt dat een voor de burger bevreesde overheid - zoals die zich steeds meer laat kennen - zorgvuldig omgaat met grondrechten, privacy en begrippen als redelijke verdenking? Van Snowden weten we dat NSA-medewerkers in de VS de tapsystemen misbruikten om hun (ex-) geliefden te stalken. We weten dat overheden van hard- en softwaremakers eisen dat die achterdeurtjes inbouwen waardoor geheime diensten in hun systemen kunnen binnen dringen.

*De toezichtcommissie die wordt ingesteld is niet per definitie betrouwbaar*. Bijvoorbeeld omdat oud-AIVD'er en uitgesproken Sleepwetvoorstander Ronald Prins er onderdeel van uitmaakt. Zijn Fox-IT is al jaren het go-to digitale security-bedrijf voor de overheid. In zekere zin was hij al jaren een soort schaduwminister van informatietechnologie. Maar los van poppetjes als Prins: sowieso zou je de overheid niet per definitie moeten vertrouwen met zo veel macht over je persoonlijke gegevens. Dat "ze" niet per se de intentie hebben om jou als nutteloze kutburger met niks te verbergen te targetten voor het slepen van je data, wil niet automatisch zeggen dat je de overheid daarom maar met de middelen moet vertrouwen om het desgewenst tóch te kunnen doen.

Het vrije internet: leuk zo lang het duurde

Langzaam groeit het gevoel en het besef dat het lang leuk was op het vrije, ongereguleerde en creatief onuitputtelijke wereldwijde web, maar dat het sleepnet van overheid (en verwoestende commercie) zich langzaam begint te sluiten om de meest vrije, open en democratische marktplaats voor ideeën waar de mens ooit op samen kwam.

We zien de desastreuze verstikking overal, in het groot en in het klein. Facebook, bijvoorbeeld, is al jarenlang een online satan die de vrijwillig gedoneerde privédata van gebruikers vermarkt aan verkopers terwijl het tegelijkertijd een zedenmoraal oplegt. Naakt? Zoenende homo's? Blote kunst? En tegenwoordig zelfs: rechtse praatjes? Je wordt weggejorist en/of opgerot - de handelswaar mag immers niet bederven. Zuckerberg wil wel je data uitzuigen maar kan je zeden niet verkopen.

We zien het ook bij Google waar een kritische medewerker - James Damore - werd ontslagen vanwege weigering om aan te conformeren aan identiteitspolitieke SJW-mores die het bedrijf in zijn (of haar of het) greep houdt, en ook bij dochter YouTube, waar migratiekritische vloggers worden gedemonetized uit naam van lege deugretoriek als 'diversiteit' en 'inclusiviteit'.

Fucking uitgelekt: de hype tegen de hyperlink

Maar Facebook kun je nog negeren, of je account opheffen als het je te gortig wordt. Voor YouTube zijn alternatieven. Veel erger is staatsbemoeienis. We zien natuurlijk al sinds Napster de krampachtigheid rond copyright. Creators hebben recht op hun knaken, daarover geen discussie. Maar als daar overheden en rechters bij komen kijken, loert niet de vrije markt, maar het censuurmonster mee. Iedereen hier herinnert zich de GS versus Playboy-zaak nog. Die zaak begon om de verwijzing, door GS, naar de publicatie van Britt Dekkers naaktplaatjes.

De zaak eindigde een paar jaar later bij het Europese Hof in Luxemburg met een strijd om het behoud van het recht op het klikken op de vrije hyperlink, die maar ten dele werd gewonnen door ons, en een oplawaai betekende voor de vrije hyperlink. Van copyrightpiraatjes naar superhelden voor de redding van het hele internet: het kon in die zaak, waarbij we nog steeds het gevoel hebben dat er naar jurisprudentie gezocht werd om openbaar linken op internet aan banden te kunnen leggen. Kijk maar naar het uploadfilter dat de EU nu aan het bouwen is, als onderdeel van grotere wetgeving over online diensten & gebruik. Internet moet en zal meer regels krijgen. Regels in de vorm van wettelijk opgelegde sociale media-censuur in Duitsland, regels waardoor online activisten in de offline wereld Engeland niet meer in komen vanwege een Foute Mening (zoals vorige week de uitgesproken edoch

verder onschuldige Amerikaanse dames Brittany Pettibone en Lauren Southern overkwam), regels in Frankrijk waarbij Macron in verkiezingstijd het internet kan afknijpen, of regels voor mediakeurmerken in de strijd tegen “nepnieuws”, een zaak waar de overheid zich verre van zou moeten houden maar waarvoor Nederland dankzij D66 nu in de EU het voortouw neemt.

Jaloerse stasi en gewillige sleepnetschapen

Het grootste probleem zit niet eens in de reguleringsdrift van de benepen overheid, maar in de internetburgers zelf. Zij zijn de sleepnetschapen die het allemaal toe laten, of zelfs actief bijdragen aan de vernietiging van hun eigen online vrijheid. Mensen die al hun persoonlijke data klakkeloos afstaan aan bedrijven als Facebook en Google, waar gebruikers het product zijn dat door die bedrijven aan adverteerders wordt verkocht, zijn medeschuldig aan een moraal waarin ‘ik heb toch niets te verbergen’ zwaarder weegt dan de mentaliteit van ‘laat me met rust en geef me mijn privacy’.

Helaas. Die mentaliteit heeft verzuimd om zich parallel aan de opkomst van het internet te ontwikkelen. Nu de slapende reuzen der analoge overheden ook door hebben gekregen dat we inmiddels digitaal zijn gaan bestaan, misbruiken ze die veel te goeder trouw van burgers om het ‘niks te verbergen’-mantra simpelweg om hen een vals gevoel van veiligheid te geven via de invoering van digitale afluistertechnieken waar de Oost-Duitse stasi jaloers op zou zijn geweest.

“U wilt toch geen aanslagen, geen kinderporno en geen radicale propaganda?”, zegt die overheid poeslief, waarop de burger gretig zijn gegevens afstaat omdat ze bang zijn van het tegendeel te worden beticht door de houders van het geweldsmonopolie.

En zo gooien we onze data nog net niet proactief maar sowieso wel vrijwillig in het sleepnet van een “beheerder” die bewezen heeft niet met ICT & data overweg te kunnen, ons niet vertelt met welke landen ze het delen of waarom (vergeet bijvoorbeeld nooit dat de EU en doodeng dictatorland Turkije nog steeds dikke vrienden zijn!), en niemand afdoende kan controleren of er veilig, zuiver of met redelijke verdenking van die datagoudmijn gebruik wordt gemaakt - dat is allemaal staatsgeheim.

Droogmolen, meelwolk & algenvijver

Als het een filmscène was, moet je denken aan een komedie waarbij agenten een boef achtervolgen door de achtertuinen van een volkswijk. Ze gaan van tuin naar tuin, over de schutting en soms door keukens, toegejuicht door brave burgers die de boef gepakt willen zien. Tijdens de achtervolging blijft er van alles aan de agenten hangen. Ondergoed van een droogmolen, een wolk bakmeel uit een keuken waar ze doorheen stormen of een paar natte broekspijpen omdat een agent de troebele algenvijver niet van de grasmat kon onderscheiden.

Dat zijn respectievelijk je naaktfoto’s, je door gesms’te drugsbestellingen en het mapje ‘Tentamenteksten’ waar in werkelijkheid je ranzigste fetishporno in verborgen zit. “Bijvangst”, heet dat in jargon. “Einde carrière”, heet het in verkeerde handen. “Recht op privacy”, heet het in termen van de Grondwet. En we geven het allemaal gratis weg.

Maar de angst voor de “domme” burger die we bij D66 zien, en de afschaffing van het referendum waarin die angst zich uit en waarmee ze de afstand tussen burger en bestuur groter maken, laat goed zien waarom de Sleepwet juist de kans op een verdere verslechtering van de relatie burger/staat zou kunnen vergroten: als we al geen directe openlijke inspraak meer mogen hebben in politieke besluitvorming omdat de staat de mening van de kiezer vreest, wie garandeert ons dan dat de staat niet meeluistert als we heimelijk (dus via mail, whatsapp of andere vormen van online communicatie) onze kritieken op de macht formuleren en delen?

Wie garandeert dat de overheid écht niet in de mailbox loert van media die over gevoelige zaken berichten, of meeluistert naar gesprekken tussen de advocaat en een cliënt die een falende lokale overheid voor de rechter daagt, of toch even via laptopcamera of smartphonemicrofoon aanschuift bij een privégesprek tussen arts en patiënt?

Making a Murderer (al dan niet by mistake)

Wie garandeert dat er in het geval van een (onterechte) verdenking van een burger niet vanuit een schuldige conclusie wordt teruggewerkt om in je browsergeschiedenis de rode vlaggetjes te zoeken die bij die conclusie passen? Making a Murderer, op Netflix, laat zien dat je ook zonder internet een eind kan komen als je iemand ergens voor wilt ophangen.

Ja, die garanties staan op papier in de wet. Die garanties geeft de minister, erewoord en op haar blauwe ogen, bij de Staatsomroep. Maar de vraag blijft staan: Waarom zouden we de overheid überhaupt moeten vertrouwen, en de staat toegang geven tot privédata die ze niet eens nodig zeggen te hebben?

Het kiezersdédain van D66 en de algemene angst voor de (mondige, kritische) burger die bij de rijksoverheid lijk te leven, zou bovendien ook zomaar kunnen verschuiven naar een angst voor specifiek de 'vreemde' burger, wanneer bijvoorbeeld een PVV aan de macht komt. De kans die er nu is om gericht te zoeken naar subversieve predikers in haatzaaiende moskeeën (en die door het 'speld in een stapel spelden'-effect van een Sleepwet wordt verspeeld) zou dan wel eens om kunnen slaan naar een algehele schending van de rechten van alle moslims, óók de brave, hardwerkende gelovige die in zijn eigen tijd 'toevallig' moslim is. De Sleepwet maakt zulke 'specificatie' van bevolkingsgroepen makkelijker - met alle potentiële gevolgen van dien.

Iedereen die na voorgaande alinea zegt dat moslims juist de reden zijn dat we wél een sleepwet nodig hebben, is zelf een sleepnetschaap - en onderdeel van het probleem. Moslim zijn mag in Nederland - gelukkig, want vrij land met vrij recht op vrije geloofsovertuiging. Wat niet mag, is uit naam van je geloof (of welke overtuiging dan ook) de democratie ondermijnen, haat zaaien en/of bloed vergieten. Mensen die dat toch willen (en dan kijken we net zo goed naar AFA en extreemlinks als naar salafisten en overig fascistoïde extreemrechts), dáár moeten de diensten zich op focussen. Dat kan prima zonder sleepwet voor alle burgers.

Het sleepnet sloopt de vrije schapenleving

Alle burgers hebben namelijk wat te verbergen, ook of zelfs juist als ze onschuldig zijn. Hun ideeën, hun uitingsvrijheid en hun creativiteit is niet per definitie voor (het morele oordeel van) de grote gemeenschap geschikt, maar daarom nog niet verdacht, te vrezen of illegaal. Het is in dezen GroenLinks dat daar het beste verhaal over heeft, via Kamerlid Kathelijne Buitenweg:

"Wat heb je te verbergen? De kern van wie ik ben! Een individu – in een vrije samenleving. Want als je weet dat de overheid je altijd kan volgen, als je merkt dat wordt meegelezen, dan heeft dat een effect op je gedrag. Bewust of onbewust zullen velen rekening houden met wat ze schrijven, welke artikelen ze lezen en welke reisschema's ze plannen. Massale surveillance van ons allemaal, dat gaat ten koste van de creatieve samenleving, dat gaat ten koste van onze innovatieve economie en dan verliezen we een stuk van onze vrijheid."

Om nog iets verder te gaan dan dit citaat: het zijn de uitersten die de samenleving spanning geven, die rek op de strek houden en die zorgen dat de grenzen aan vrijheden zo ver mogelijk bij ons vandaan worden gelegd en gehouden. Je hebt wel diensten nodig die zorgen dat die grenzen worden bewaakt, maar die dienen enkel áán die grenzen te opereren. Niet net daarbinnen. En al helemaal niet in het middenveld.

Een raster langs de randen, dat moeten onze diensten zijn. Geen sleepnet over de hele samenleving. Maar enfin. Te laat. Analoog leven gaat uiteindelijk nog eens heel groot worden.

**Privacy Barometer: 'De sleepwet is niet effectief, intimiderend en onrechtmatig'**

Bits of Freedom, de Piratenpartij, de Partij voor de Dieren, de SP, Forum voor Democratie, zelfs Amnesty International steunen een sleepwetreferendum. Maar daarmee zijn die krabbels nog niet binnen. Dus hier volgt een persbericht van Privacy Barometer.

De nieuwe sleepwet geeft geheime diensten verregaande bevoegdheden die niet effectief zijn in de strijd tegen terrorisme. Wel zijn de bevoegdheden intimiderend en zelfs onrechtmatig. Om die reden is een referendum over de wenselijkheid van deze sleepwet dringend noodzakelijk.

Met de nieuwe sleepwet mogen de inlichtingendiensten grootschalig het internet afluisteren, meekijken wat u doet op WhatsApp, Twitter of Facebook en deze afgeluisterde gegevens drie jaar bewaren. Ze mogen gegevens die bedrijven en (zorg-)instellingen van u hebben automatisch aftappen en elektronische apparaten hacken zoals laptops, mobieltjes, slimme meters en zelfs pacemakers. Al deze gegevens mogen aan elkaar gekoppeld worden en met profielen worden doorzocht. De gegevens mogen ook gebruikt worden om misdrijven op te sporen en om met buitenlandse inlichtingendiensten te delen.

Op dit moment worden 300.000 handtekeningen verzameld voor een referendum. Via een referendum zou de Nederlandse bevolking zich kunnen uitspreken of we deze verregaande bevoegdheden in onze vrije samenleving zien zitten. Dat is nodig vanwege de onderstaande grote problemen met deze wet.

Niet effectief

Grootschalig afluisteren is niet effectief. Bij de meeste aanslagen blijken de daders bekend te zijn bij inlichtingendiensten of bekend te staan als jihadist. Potentiële aanslagplegers die al bekend zijn, hoeft men niet op te sporen door grootschalig het internet af te luisteren. Ook onder de huidige wetgeving is het al mogelijk gericht verdachte personen op internet af te luisteren.

Bij de laatste aanslagen in Barcelona hebben de daders offline gecommuniceerd juist om ontdekking te voorkomen. De aandacht voor dergelijke dreigingen kan verslappen als de AIVD druk is met het afluisteren van de rest van Nederland.

De Raad van Europa heeft onderzoek gedaan naar grootschalig afluisteren en concludeert onomwonden dat "massasurveillance geen effectief middel is in de strijd tegen terrorisme of georganiseerde misdaad in vergelijking met traditionele, gerichte surveillance".

Ook het doorzoeken van gegevens met profielen om terroristen te vinden is niet effectief. De Wetenschappelijke Raad voor het Regeringsbeleid constateert: "Omdat elke terroristische aanslag uniek is, is het nagenoeg onmogelijk om een goed profiel te maken. In combinatie met een gering aantal aanslagen levert dit te hoge foutpercentages op."

*Gebrekkig toezicht*

Verregaande bevoegdheden verdienen extra goed toezicht. Dat ontbreekt in deze wet. Voor de bevoegdheden moet een speciale commissie toestemming geven, maar die mag niet alle informatie inzien en kan daarom onmogelijk een afgewogen oordeel geven. Achteraf mag de toezichthouder CTIVD de inlichtingendiensten controleren, maar die mag weer geen bindende adviezen geven.

Instanties als de Raad van State, de CTIVD en de Autoriteit Persoonsgegevens hebben er op gewezen dat het toezicht onder de maat is. Met die kritiek is niets gedaan.

Intimiderend

Er gaat een intimiderende werking van de wet uit. Grootschalig afluisteren van internet zal mensen voorzichtiger maken. U weet immers nooit of de autoriteiten meekijken bij wat u op internet doet. Een onderzoek van de universiteit van Californië laat zien dat na de Snowden-onthullingen, pagina's met terrorisme-gerelateerde onderwerpen 20% minder werden bezocht. Een ander onderzoek laat zien dat 34% van de mensen terughoudender op internet wordt door het grootschalig afluisteren. Volgens de onderzoekster "dwingt de angst voor overheidscontrole tot een vorm van zelfcensuur die we normaal in politiestaten zien".

Economische schade

Volgens Nederland ICT, de brancheverenigingvan de ICT sector die bijna € 30 miljard omzet en meer dan 250.000 medewerkers telt, is de nieuwe wet "funest" voor het internationale vertrouwen. "De economische schade door het verlies aan vertrouwen in digitale diensten [na de onthullingen door Snowden] was in de VS groot. Het is zeer onwaarschijnlijk dat dit in Nederland anders zal zijn."

In strijd met mensenrechten

Ongerichte massa-surveillance is in strijd met fundamentele mensenrechten. Afluisteren van mensen is alleen toegestaan als het duidelijk is afgebakend, zowel in tijd als in categorieën personen. Het Europese Hof heeft in 2008 het grootschalig afluisteren door de Britse regering vanwege het abstracte begrip "nationale veiligheid" als onrechtmatig bestempeld.

Totalitaire infrastructuur

Met de nieuwe wet wordt een infrastructuur opgetuigd om de gehele bevolking in de gaten te houden. Er komen aftappunten bij internetknooppunten en mogelijk bij (tech-)bedrijven of instellingen. Er komen grote opslagsystemen bij de AIVD en software om alle gegevens van Nederlanders te koppelen en analyseren. Dit is de infrastructuur die je verwacht in totalitaire regimes. Ook democratisch gekozen leiders kunnen die infrastructuur inzetten voor eigen doelen, zoals bijvoorbeeld de Turkse situatie laat zien.

Teken ook voor een referendum

Nederland zou zich sterk moeten verzetten tegen deze ontwikkelingen, of zou in ieder geval mee moeten kunnen beslissen of we dit willen. Daarom verdient deze wet een referendum. Vindt u ook dat burgers zich zouden moeten uitspreken over deze verregaande bevoegdheden van onze geheime diensten? Tot en met 16 oktober 2017 kunt u de oproep voor een referendum hier tekenen. U kunt ook direct uw handtekening naar de Kiesraad opsturen. Daarvoor kunt u hier het formulier en adres vinden.

**Red de democratie, stop de Sleepwet! – Jelle de Graaf – JOOP!**

'De digitale revolutie mag er niet voor zorgen dat verworvenheden van eeuwen verloren gaan. Het is de verantwoordelijkheid van de leiders van deze generatie om burgerrechten ook in de 21e eeuw te beschermen. Als ze dat niet uit zichzelf doen is het onze verantwoordelijkheid ze daartoe te dwingen'

Politici hebben de neiging apocalyptisch over te komen. Toch zal ik vandaag ook een duit in het zakje doen. Want de democratie ligt onder vuur. Ik heb het niet over het gewelddadige neerslaan van

vreedzame protesten in Barcelona, of de bedreiging van de rechtstaat door nationalistisch-rechtse partijen in het Nederlandse parlement, maar over een wet die eerder dit jaar stilletjes werd aangenomen door een ruime meerderheid van de traditionele partijen. Haar officiële naam is de vernieuwde Wet op de Inlichtingen en Veiligheidsdiensten maar hij staat beter bekend als de Sleepnetwet of de Sleepwet. Dit referendum geeft ons een tweede kans deze bedreiging voor de democratie af te wenden.

De Sleepwet geeft de inlichtingendiensten de mogelijkheid om al het internetverkeer in Nederland ongericht – als met een sleepnet – af te luisteren, apparaten te hacken, de gegevens die ze hiermee verzameld drie jaar te bewaren, deze gegevens zonder ze ook maar te bekijken te delen met buitenlandse inlichtingendiensten en dit alles zonder dat er een rechter aan te pas komt.

Het grootschalig, ongericht verzamelen van internetverkeer van mensen die nergens van verdacht worden is een grove en disproportionele inbreuk op de privacy. Het opslaan van die gegevens voor drie jaar lang, een extreme tijd in vergelijking met andere landen, is een onnodig gevaar. Ook is het ongericht aftappen van grote hoeveelheden informatie helemaal niet effectief voor het voorkomen van terroristische aanslagen. Hoe vaak hebben we niet al gehoord dat de dader van een aanslag in zicht was bij de diensten? Het probleem is niet dat geheime diensten te weinig informatie hebben, het probleem is dat het ze niet lukt uit bergen gegevens de juiste informatie te halen.

Een onnodig grote, langdurige en disproportionele inbreuk op de privacy en een gebrek aan effectiviteit zijn grote kritiekpunten en het is logisch dat het debat over de Sleepwet zich daarop heeft gefocust. Maar er zijn manieren waarop de Sleepwet de democratie fundamenteel aantast waar nog minder aandacht voor is geweest.

In de Sleepwet is het niet een rechter, maar de minister die bepaalt welke gegevens wanneer worden verzameld. Hiermee wordt ruw een einde gemaakt aan de scheiding der machten. Machtsmisbruik ligt hiermee op de loer. Hoe kunnen we erop vertrouwen dat een minister goed zijn eigen werk controleert? *In de nieuwe wet mag de toezichthouder op de diensten weliswaar toezicht houden tijdens het aftappen en eventueel advies geven, maar de minister kan dit net zo makkelijk naast zich neerleggen. Aftappen zou niet alleen altijd gericht moeten gebeuren, maar ook altijd onafhankelijk getoetst.*

Een ander groot gevolg van de Sleepwet is dat journalisten, de onafhankelijke hoeders van onze democratie, hun bronnen geen bescherming kunnen garanderen. De gesprekken die journalisten voeren kunnen bewust worden afgeluisterd. Dat de diensten hiertoe bereid zijn bleek toen journalisten van de Telegraaf maandenlang werden afgeluisterd, tot de rechter hier uiteindelijk een stokje voor stak. Ook kan communicatie van journalisten, om in de vissersterminologie te blijven, als ‘bijvangst’ in handen van de diensten terecht komen. Over bijvangst zei minister Plasterk eerder: “We bedoelen geen tasjesdieven.” Het stelt mij niet gerust.

Als laatste wil ik stilstaan bij het gevaar van zelfcensuur. Vrije, kritische en onafhankelijk denkende burgers vormen de basis van een functionerende democratie. In de kern gaat democratie over de machtsverhouding tussen een bevolking en haar bestuur. Als die bevolking op elk moment over haar schouder moet kijken omdat haar regering misschien meeluistert is de kans groot dat afwijkende meningen zich niet of minder snel ontwikkelen.

Ben je wakker? Mooi. Niet alleen is een coalitie van maatschappelijke organisaties bezig met een rechtszaak om te kijken de Sleepwet wel mag volgens het Europees Verdrag voor de Rechten van de Mens, ook jij kan iets doen. Een betrokken groep studenten is keihard bezig een raadgevend referendum over de Sleepwet af te dwingen. Hoe je ook over referenda denkt, ik roep je van harte op dit referendum te steunen.

Ik kan me het dilemma voorstellen van partijen als GroenLinks en D66 die in de Kamer tegen de Sleepwet stemden, maar dit referendum niet steunen omdat ze tegen referenda zijn. Zoals een collega-Piraat ooit zei over referenda tegenover echte democratische vernieuwing: “Ik wil geen noodrem, ik wil kunnen sturen.” Maar als de democratie onder vuur ligt zijn alle middelen geoorloofd. Het behouden van democratische kernwaarden heeft nu even voorrang op het verdiepen van de democratie.

Ook in het digitale tijdperk moeten de politie en diensten hun werk goed kunnen doen. Als de Wet op de Diensten daarvoor moet worden aangepast is dat zo, maar de digitale revolutie mag er niet voor zorgen dat verworvenheden van eeuwen verloren gaan. Het is de verantwoordelijkheid van de leiders van deze generatie om burgerrechten ook in de 21e eeuw te beschermen. Als ze dat niet uit zichzelf doen is het onze verantwoordelijkheid ze daartoe te dwingen.

**Ollongren vertelt zelf waarom U tegen de sleepwet moet stemmen**

Ga ervan uit dat in de ogen van de overheid geen enkele burger onschuldig is.

Dinsdagavond gaf minister Kasja Ollongren zélf het beste argument om tégen de sleepwet te stemmen. Zij verklaarde dat de inlichtingendiensten in het geheel niet geïnteresseerd waren in informatie van onschuldige burgers

Dat is een opmerking om je grote zorgen over te maken. Zulke diensten hebben immers allemaal hun eigen opvattingen over schuld en onschuld. *Zij worden door de commissie Stiekem van de Tweede Kamer zeer onvoldoende gecontroleerd en zij laten ook tegenover de verantwoordelijke ministers het achterste van hun tong niet zien.* Wat landsbelang is en wie dit bedreigen, bepalen zij in hogen mate zelf. Dat is al het geval sinds mr. Louis Einthoven, oud commissaris van politie te Rotterdam en tijdens de bezetting mede-initiatiefnemer van de Nederlandsche Unie, de Binnenlandse Veiligheidsdienst uitbouwde, oermoeder van de tegenwoordige AIVD. Hij was demother van de Nederlandse James Bonds, die in zijn tijd overal het communisme roken. Tegenwoordig snuift men enigszins andere geuren op maar het wantrouwen gaat toch nog vooral uit naar links en het uitheemse.

Veel Nederlanders denken dat zij niets te verbergen hebben. Zij gaan elke dag netjes naar hun werk. Zij zijn niet geïnteresseerd in radicaal islamistisch gedachtengoed en evenmin zijn zij geïnteresseerd in plaatjes met kinderseks. Daarom denken zij dat hun surfgedrag geen wantrouwen kan opwekken bij wat dan heet “de diensten”. Dit is een verschrikkelijke misvatting. Of zulk surfgedrag verdacht is, hangt af van de hoeveelheid paranoia waarmee de opbrengst van het sleepnet wordt geanalyseerd. Het kan bijvoorbeeld best zijn dat U voor de aardigheid wel eens politiek verdachte sites hebt bezocht van linkse of rechtse snit, terwijl U – blijkt uit beelden van bewakingscamera´s ook op het verkeerde moment in de verkeerde buurt hebt gewandeld, misschien zelfs met de verkeerde kleren aan zoals een hoofddoek. Was U op weg naar een haatpreek of een radicale vergadering? Waarom had U juist nú Uw mobieltje thuis gelaten? Of wilde U zich aansluiten bij de optocht van Pegida? Gaat U wel vaker naar bijeenkomsten met de heer Baudet waarin hij het voor Rusland opneemt? Of moest U bij de Internationale Socialisten zijn? Wat deed U in de buurt van het Piet Hein beeld net nadat het beklad is. Moest U misschien op de uitkijk staan?

U zegt: de AIVD en de MIVD, dat zijn geen Stasi-achtige organisaties. Het is hier de DDR niet. Toch hebben we al te maken met een overheid die verbijsterend veel informatie over U verzamelt en ook combineert. Hoe zit dat met die vakanties in Cilicië, zogenaamd om daar in de bergen te wandelen? Wie wandelde mee?

U kunt zichzelf wel onschuldig vinden maar de diensten kijken verder, schouwen dieper.

In tegenstelling tot sommige lezers van Joop, die straks daarover een reactie zullen schrijven, zie ik minister Ollongren noch haar collega Bijleveld er voor aan dat zij een heksenjacht openen op

potentieel subversieve elementen in Nederland maar wij weten niet wie haar opvolgers zijn. Wij tuigen in Nederland een controle- en surveillancesysteem op dat goud waard is in de handen van bestuurders die weinig op hebben met democratie en vrijheid. Bedenk hoe verschrikkelijk veel plezier de Duitse bezetters hebben gehad van de voortreffelijke Nederlandse bevolkingsadministratie: alle burgers waren met naam, toenaam, adres, leeftijd en levensovertuiging bij de autoriteiten bekend. Je hoefde de politie maar langs te sturen om ze op te halen.

Ga er van uit dat in de ogen van de macht geen enkele burger onschuldig is. En als U dat niet gelooft, bedenk dan hoeveel controlemechanismes de overheid de laatste decennia heeft opgetuigd om de burger te volgen en te betrappen op misstapjes. Kijk naar de volstrekt uit de hand gelopen rapportageplicht die aan professionals zoals artsen en leraren is opgelegd. Observeer de handhaverij van dorpspotentaatjes in heel het land.

Stem tegen de sleepwet. Neem die moeite. Laat U niet ontmoedigen door de overtuiging dat Den Haag het resultaat toch in de prullenbak gooit. Al was het alleen maar omdat het dan niet aan U gelegen heeft als straks alles misloopt. En als U dan nóg niet overtuigd bent, doe dan even U ogen dicht en stel U voor dat de politicus, die U het diepste haat en wantrouwt, in het Torentje zetelt. Wat zal die doen met een Sleepwet die mede door uw lamlendigheid tot stand is gekomen? Haal dat maar eens voor de geest.

**VICE: 5 redenen dat je tegen de sleepwet moet stemmen**

De sleepwet geeft geheime diensten ronduit creepy mogelijkheden om ons online in het oog te houden. Al onze elektronische apparaten mogen gehackt worden, en wat ze vinden, mogen ze 3 jaar bijhouden. Ons redden voor mogelijke aanslagen zal het niet, want terroristen communiceren ondertussen bewust offline.

Mocht je nog niet precies weten wat de Sleepwet inhoudt, we schreven er eerder ook al over.

Een groepje studenten, over wie we kortgeleden schreven, zorgde daarom dat er een werd afgedwongen. Voor 16 oktober moesten dat er 300.000 zijn en dat is gelukt, en nu gaat het referendum ook door.

1. Deze wet doet niet wat hij belooft

Bij de meeste aanslagen bleken de daders al bekend te zijn bij inlichtingendiensten, want verrassing: er bestaan al wetten om verdachte personen af te luisteren. Waarom zou je dan iedereen willen afluisteren?

De Raad van Europa is in een onderzoek heel duidelijk: "massa surveillance is geen effectief middel in de strijd tegen terrorisme of georganiseerde misdaad in vergelijking met traditionele, gerichte surveillance." Focus op de bad guys, lieve politiemannen en -vrouwen.

Volgens De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) is het ook niet zinvol om massaal profielen te doorzoeken om terroristen te vinden: "Omdat elke terroristische aanslag uniek is, is het nagenoeg onmogelijk om een goed profiel te maken." De WRR vindt de kans op fouten gewoon te hoog.

2. Deze wet zorgt voor veel gestalk, maar weinig toezicht

Bij zo'n extreem stalkerig gedrag van de overheid verwacht je extra goed toezicht. Dat is er niet in deze wet. Er is wel een speciale commissie die haar toestemming moet geven voor het afluisteren, maar die krijgt niet alle informatie. Dat maakt het onmogelijk om een genuanceerd oordeel te vellen. *Instanties als de Raad van State, de CTIVD en de Autoriteit Persoonsgegevens hebben er op gewezen dat het toezicht ondermaats is*. Met die kritiek werd niets gedaan.

3. Deze wet is intimiderend en zorgt voor zelfcensuur

Als ik weet dat ik constant afgeluisterd kan worden, zou ik veel dingen niet meer zo snel doen. Zelfs mogelijks onschuldige dingen, zoals "how to get away with murder" googlen worden dan een beetje scary. Dat is gewoon een Amerikaanse serie, maar je weet maar nooit.

Een onderzoek van de universiteit van Californië laat zien dat na de Snowden-onthullingen pagina's met terrorisme-gerelateerde onderwerpen 20% minder werden bezocht. Een ander onderzoek laat zien dat 34% van de mensen terughoudender wordt op internet als ze weten dat ze grootschalig afgeluisterd worden. De angst voor gevolgen "dwingt mensen tot een vorm van zelfcensuur die we normaal in politiestaten zien," schrijven de onderzoekers.

4. Deze wet is niet goed voor de economie

Volgens brancheverenigingNederland ICT (bijna € 30 miljard omzet en meer dan 250.000 medewerkers) is de nieuwe wet catastrofaal voor het internationale vertrouwen. Na de onthullingen van Snowden zorgde dat voor grote economische schade in de VS. "Het is zeer onwaarschijnlijk dat dit in Nederland anders zal zijn," besluit Nederland ICT.

5. Deze wet maakt inbreuk op onze mensenrechten

Ongerichte massa-surveillance is in strijd met fundamentele mensenrechten, zoals het recht op privacy en privéleven dat elke mens bezit. Mensen afluisteren mag enkel in uitzonderlijke gevallen, en voor beperkte tijd. Wanneer je, zoals de Britse regering, dat grootschalige afluisteren enkel motiveert met

een abstract begrip zoals "nationale veiligheid" – zal je wet vroeg of laat door het Europese Hof als onrechtmatig worden bestempeld. Maar dat kan vermeden worden, door zo'n wet te voorkomen.

Lijkt de sleepwet je niks? De oproep voor het referendum kan je hier ondertekenen.

**De sleepwet gaat speurwerk alleen maar onoverzichtelijker maken**

Op donderdag 14 december komt Ben Makuch, de presentator van Cyberwar, op ons hoofdkantoor in Amsterdam langs om te praten over cyberoorlog.Wil je ook aanwezig zijn? Meld je dan hier aan.

“Met de Sleepwet zullen we er technisch gezien niet erg op vooruit gaan. Hoe meer informatie, hoe meer big data je verzamelt, hoe lastiger het zal worden om de boef te vinden,” schrijft hoogleraar softwaretechnologie Marko van Eekelen zelfzeker in een recent nieuwsbericht van de Open Universiteit. Hij herhaalt: “Hoe meer hooi je op de hooiberg gooit, hoe lastiger het wordt om de speld te vinden”. Zijn onze inlichtingendiensten de zoveelste slachtoffers van data-overload?

“We willen geen hooi toevoegen, maar weghalen,” zegt een woordvoerder van de AIVD via de telefoon. “Op zoveel mogelijk informatie zitten we niet te wachten. Daarom zoeken wij gericht naar dreigingen, en proberen we dan zo snel mogelijk naar de kern te gaan.” De diensten zullen dankzij de Sleepwet toegang tot veel meer data krijgen, maar er naar eigen zeggen slechts een kleiner, overzichtelijk (gericht) deel van gebruiken.

De woordvoerder vertelt dat de diensten namelijk niet elk appje gaan lezen dat in Nederland verstuurd wordt, maar enkel het internetverkeer aftappen (via de kabel) in de wijk van iemand die ze al op het oog hebben. Ze halen de metadata binnen: bijvoorbeeld wie met wie chat, maar niet de inhoud van het gesprek, en beperken zich indien mogelijk tot de relevante telefoonnummers en ip-adressen. Zo kunnen ze eventueel dus zien dat jij met je beste vriend chat, maar niet dat je net vertelde dat dat je een gigantische kater hebt. Pas wanneer ze een verdachte op het spoor zijn, mogen de inlichtingendiensten de gespreksinhoud bekijken. “Het gaat om heel gericht onderzoek, niet om het doorspitten van allerlei data,” zegt hij.

Gericht zoeken versus veel data doorspitten: volgens Rejo Zenger is dat een valse tegenstelling. Hij is beleidsadviseur bij digitale burgerrechtenbeweging Bits of Freedom, en schrijft al jaren over privacykwesties bij de politie. Via de telefoon vertelt hij: “Als je een hele wijk aftapt, zul je toch gigantisch veel gegevens verzamelen, ook al is dat enkel metadata. Hoe gericht je uiteindelijk ook zoekt, eerst moet je al die metadata doorspitten.”

Vorig jaar kreeg de NOS een vertrouwelijk document van de AIVD in handen dat een concreet beeld geeft van een internettap onder de Sleepwet. In het document vraagt de AIVD internetproviders hoeveel het zou kosten om in een stad van 400.000 inwoners al het internetverkeer te onderscheppen van mensen die een bepaalde chatdienst gebruiken. Je weet wel, zo’n kleine, overzichtelijke wijk van bijna een half miljoen mensen.

In het document schrijft de AIVD dat ze zo maximaal de gegevens van 200 mensen zullen onderscheppen. Veel versleutelde chatdiensten, zoals Telegram, Signal of Cryptocat, zijn ontzettend populair. En bijna elke week krijg je wel weer deze notificatie: “is nu actief op Telegram.” Dus steeds meer mensen gebruiken versleutelde chatapps. "We hebben de indruk dat ze het aantal mensen [dat kan worden afgetapt] proberen te downplayen," zegt een anonieme medewerker uit de telecomindustrie, die veel te maken heeft met het aftappen van netwerken, tegen de NOS.

Op Skype vraagt prof Van Eekelen zich nog steeds af of dat aftappen van online (meta)data de beste oplossing is: “Ik kan je geen wetenschappelijk bewijs geven, maar in de krant lees ik na een aanslag vaak: ‘de daders waren bekend bij de autoriteiten’. Daardoor vraag ik me af: hoe effectief is die massaverzameling van gegevens eigenlijk? Als ze de daders kenden, maar hen toch niet konden tegengehouden... dan ben je niet veel met al die data.”

Hoe effectief zou de Sleepwet zijn als deze er komt? Die vraag is niet zo gemakkelijk beantwoorden, omdat de werking van geheime diensten nogal eh... geheim is. Tijd om eens te kijken naar gelekte gegevens van klokkenluiders en nationale onderzoeksrapporten na aanslagen.

Laten we beginnen met Snowden. The Intercept publiceerde een stuk over zijn onthullingen met de grafiek hier boven. Die laat zien dat de Britse geheime dienst MI5 in 2008 en 2009 vijf miljoen oproepen, berichten en andere data heeft onderschept. Opvallend is dat 97% van de gegevens niet bekeken werd. “Er is een wanverhouding tussen de verzameling en de uiteindelijke benutting van de data”, klinkt het in het rapport van MI5. De oorzaak? “Een gebrek aan personeel en tools. Het materiaal werd niet volledig benut, omdat de evaluatie ervan aanzienlijk veel tijd kost.” Dan kom je niet ver met al die data, zou Van Eekelen zeggen.

Net zoals in het Verenigd Koninkrijk hebben ook de Belgische veiligheidsdiensten te weinig personeel voor hun data-inspanningen. “Ze hebben steen en been geklaagd omdat ze geen analisten hadden”, vertelt de Belgische advocaat Jos Vander Velpen via de telefoon. “Ondertussen is er meer personeel, maar dat gaat maar mondjesmaat. Competente werknemers zijn duur.” Ook de Nederlandse AIVD en MIVD zijn meer technisch personeel aan het aanwerven: op dit moment staan er bij hen 13 tech-vacatures open, met titels zoals ‘big data engineer’.

Volgens Vander Velpen, voorzitter van de Belgische Liga voor Mensenrechten, wordt de effectiviteit van massasurveillance overdreven. “Alles wordt ingezet op high tech, op buitensporige investeringen, die heel veel informatie opleveren. Daarin verdwijnt de echt nuttige informatie dan,” zei hij eerder dit jaar op een conferentie over de nieuwe veiligheidswetten en -maatregelen in Brussel.

“Ondertussen kiest men niet voor de echt efficiënte aanpak: investeren in mensen, in onderzoekswerk, in preventie. Het aloude 'detectivewerk' is nog altijd de beste oplossing,” ging hij verder. Die uitspraken baseert Vander Velpen op een recent verschenen parlementair onderzoek naar de omstandigheden die hebben geleid tot de terroristische aanslagen van 22 maart 2016 in Brussel.

“Elektronische onderschepping heeft toen nauwelijks iets opgebracht: het heeft de daders niet in beeld kunnen brengen. Verder waren er ernstige tekortkomingen in het klassieke, menselijke onderzoekswerk, zoals infiltranten of informanten. Die zijn nauwelijks gebruikt geweest, hoewel dat nu net voor de hand liggend was,” zegt Vander Velpen.

“Om de daders van de aanslagen in Brussel [tegen te houden], heb je geen computers nodig, maar vooral de ogen en oren van [de politie in de buurt]”, zegt Vander Velpen. “Het is een groot gemis dat die gemeenschapsgerichte politie voor een groot stuk is afgebouwd. Die leegte werd dan opgevuld met de magische formule van massasurveillance.“

Ook in Frankrijk zijn er te weinig politiemannen en -vrouwen op straat. The Guardian schreef na de aanslagen in Parijs in 2015: “Franse veiligheidsdiensten en politie hebben tussen de 500 à 600 agenten om mensen fysiek te volgen. Maar daartegenover staan ongeveer 11.000 mensen die geïdentificeerd zijn als mogelijke bedreiging voor de nationale veiligheid.” Eén persoon schaduwen doen ze met een

groep van 30 à 40 politiemensen. Als je maar 20 verdachten in heel Frankrijk kan schaduwen, wordt kiezen al snel heel letterlijk verliezen.

Een aanvulling hierop is dat de AIVD en MIVD meer doen dan alleen terroristen volgen. Ze monitoren ook cyberaanvallen en houden zich bezig met spionage van landen zoals China en Rusland. Informatie, ook die van terroristen, gaat voor een belangrijk deel via de kabel - niet de telefoon, maar het internet. Door de Nieuwe Wet op de inlichtingen- en veiligheidsdiensten (De Wiv, zoals de sleepwet officieel heet) hopen de inlichtingendiensten ook daarop meer zicht te krijgen. Het gevaar dreigt anders dat de Nederlandse inlichtingendiensten overklast worden.

Toch wijst Rejo Zenger van Bits of Freedom erop dat de daders van aanslagen telkens bekend waren bij de Nederlandse autoriteiten, maar niet meer gevolgd werden. “Dat pleit er volgens mij voor dat de diensten slimmer moeten omgaan met de gegevens die ze hebben, want blijkbaar waren die daders al in beeld. Daarom moeten we meer investeren in slimmer onderzoek, en niet perse in het toevoegen van meer gegevens. Het kost misschien meer tijd om met mensen te werken, maar ik denk dat je zo heel goed werk kan doen.”

Hij vindt het belangrijk dat de inlichtingendiensten goed kunnen aanvoelen hoe verdachten denken. “Je zult te weten moeten komen wat de waarden van iemand zijn. Zo kom je bijvoorbeeld te weten of iemand die aan het radicaliseren is ook werkelijk een gevaar vormt.” Dat doe je volgens hem met behulp van de juiste contacten en degelijk menselijk werk.

Die visie bevestigen politiedeskundigen Teun Meurs en Jan Kreulen in hun artikel over ‘gebiedsgebonden politiezorg’ in de een recente editie van vakblad Justitiële verkenningen. Wijkagenten hebben het blijkbaar vaak nog moeilijk met aanvoelen of iemand aan het radicaliseren is of dat er iets anders aan de hand is: “De interacties tussen burgers en politieagenten verlopen geregeld moeizaam en met wederzijds onbegrip.” Vooral in steden is het politiewerk volgens hen complexer geworden, omdat agenten moeten kunnen omgaan met ‘superdiversiteit’: inwoners met allerlei verschillende landen van herkomst, culturen en religies. “Journalist en Arabist Maarten Zeegers geeft in zijn boek over de moslimgemeenschap in de Transvaal in Den Haag een inkijk in dit complexe werkterrein. Hij laat zien dat het niet vanzelfsprekend is dat de politie effectief omgaat met de diversiteit in de wijk.”

Volgens Rejo Zenger werken overheden volgens het motto beschikbaarheid creëert behoefte: “Omdat big data bestaat, wil de overheid die gebruiken. Hetzelfde geldt voor slimme camera's.” Over de AIVD en MIVD kan hij geen zekere uitspraken doen, omdat ze in het geheim opereren. “Maar bij de Nederlandse politie weet ik het zeker,” zegt Zenger, “Daar worden allerlei technologieën ingezet waarvan het niet duidelijk is of ze werkelijk een meerwaarde hebben voor het politiewerk. Maar omdat de technologie bestaat, en cool is, wordt deze ingezet. Het zou me niet verrassen als iets soortgelijks ook bij de geheime diensten speelt.” Zijn conclusie? “Ik denk dat de geheime diensten de bestaande middelen beter moeten leren gebruiken, in plaats van nieuwe maatregelen te eisen die haaks staan op de waarden van onze rechtsstaat.”

**Teksten Krantenartikelen NexisUni**

**Leon de Winter – Nog even, en Orwell's 1984 is een feit – 20 maart 2018 – De Telegraaf**

China overweegt het Sociale Krediet Systeem in te voeren. Veel landen kennen al een systeem waarmee banken de financiële kredietwaardigheid van burgers meten, maar de Chinese zieners van de alwetende Communistische Partij breiden dat uit met het wegen en meten van sociaal gedrag.
Reuters meldde vorige week dat Chinezen die afwijkend gedrag vertonen, zoals roken waar dat niet mag of het verspreiden van fake nieuws, gestraft worden met een verbod op het gebruik van de trein of het vliegtuig. Het systeem schijnt al stilletjes te zijn ingevoerd; inmiddels staan zes miljoen mensen op de zwarte lijst.
We zien dezelfde tendens in het vrije Westen. Het antwoord op de volgende vraag bepaalt de score van je sociale status in het politiek-correcte Westen: draag je bij aan zowel sociale en culturele

diversiteit als aan het terugdringen van CO2-uitstoot? Wie in daad en gedachte afwijkt van de gehanteerde normen, krijgt nu al nauwelijks ruimte in het publieke debat en is een ontkenner (denk aan 'holocaustontkenner') en/of racist.
Sinds de jaren zeventig wordt het publieke debat beheerst door een sociaal-cultureel complex van linkse media en linkse politici. De mensen die daarin functioneren, behoren tot homogene sociaal-culturele groepen en vinden bij elkaar herkenning, waardering, bescherming. Ze beheersen politieke en bestuursorganisaties, ze maken de kranten, de nieuwsprogramma's op TV, de talkshows, geven elkaar subsidies, prijzen, baantjes; het is daar zo goed als onmogelijk om 'diversiteit' en de noodzaak van 'klimaatbeheersing' op kritische wijze te bespreken.
Kort geleden kreeg klimaatdissident en chemicus Marcel Crok een groot interview in de Volkskrant. Dat was moedig van de redacteur die dat deed, en van de eindredacteuren die dat toelieten. Een golf van kritiek overspoelde de Volkskrant. De meeste lezers van die krant wensen geen confrontatie met klimaatdissidenten want ze geloven, na decennia van eenzijdige berichtgeving, dat een klimaatdissident per definitie een misdadige fraudeur is, en de redactie is zich daarvan scherp bewust. Crok zal nooit meer aan het woord komen in die krant.
Maar: het internet heeft de publieke ruimte gedigitaliseerd en ten diepste gedemocratiseerd. Tot voor kort werd de toegang tot het publieke debat beheerst door organisaties van professionele redacteuren. Betreed een moment de nieuwe digitale media en het is duidelijk dat daar geen redacteuren optreden. Veel van wat daar gebeurt, is goor, weerzinwekkend, verontrustend. Maar er gebeurt ook veel wat schitterend en nieuw is. Voor mij is het een verademing want het internet heeft de autoritaire en ideologische grenzen van het publieke debat doorbroken.
De elites vechten fel terug en zetten de digitale media onder druk. In Duitsland zijn er al wetten ingevoerd die Twitter, Facebook en Google ertoe dwingen, op straffe van kolossale boetes, bijdragen op hun sites te onderzoeken op onwelgevallige ideeën. Volstrekt eerbare, eigenzinnige sites die niet de officiële diversiteits- en klimaatorthodoxie volgen (zoals de Duitse site Achgut van de befaamde journalist Henryk Broder), worden afgesloten van adverteerders en dus van inkomsten. Er woedt op het internet een gevecht om vrijheid van meningsuiting tussen traditionele machthebbers en ongebonden internetgebruikers.
Maar dit is niet alles. Er gebeurt veel meer op dat internet dat ons zorgen zou moeten baren: ons internetgedrag, zoals zoekopdrachten, wordt onafgebroken gemonitord en geanalyseerd door gigantische, gezichtloze bedrijven. Facebook en Google verdienen fortuinen aan die analyses. Via digitale systemen wordt ons gedrag in het oog gehouden: in supermarkten, trein- en busstations, zorgverzekeringen, straks via een 'black box' in de auto, via onze betaal- en creditkaarten, bewakingscamera's, de GPS-functie van onze telefoons. Op een fataal moment zullen al die systemen aan elkaar gekoppeld worden teneinde ons tot gedrag en gedachten te dwingen die volgens de elites wenselijk zijn. De wereld van George Orwells 1984 is dan een feit.
In dit fundamentele gevecht om controle over internetcommunicatie en, uiteindelijk, onze authenticiteit en autonomie, is de **Sleepwet** waarover u vandaag via een raadgevend referendum uw stem kunt laten horen, geen geïsoleerd verschijnsel. De opstellers van die wet hebben aan diversiteit en klimaatbeheersing een derde begrip toegevoegd, waarmee het zwaarste argument op tafel komt dat politici kunnen uitspelen: de staatsveiligheid. Daarvoor moet vanzelfsprekend alles wijken.
Wat u vandaag ook stemt, stem in ieder geval tegen de **Sleepwet**, die opsporingsdiensten toegang geeft tot al onze communicatie en deze ook zonder controle kan overdragen aan buitenlandse mogendheden. Telefoons en computers worden in ons land al volop getapt, en onze nationale veiligheid wordt door de bestaande regelingen niet verzwakt. Op een dag zal deze **Sleepwet** tegen ons ingezet worden omdat we, bijvoorbeeld, ouderwetse ideeën hebben over man-vrouwverhoudingen of over wat dan ook dat activistische elites onaanvaardbaar vinden. De **Sleepwet** moet vervangen worden door een wet die wel voldoende waarborgen tegen misbruik biedt. Ben benieuwd hoe de elites op een massale afwijzing zullen reageren.
De overheid staat niet boven de partijen maar is een partij. En het is de machtigste, en dus soms gevaarlijkste, partij die de samenleving kent. Tegen de **Sleepwet**.
Afwijkende gedachten afgestraft

**Rob Hoogland – Big Brother – 20 maart 2018 – De Telegraaf**

En wij de laatste tijd maar steggelen over de **Sleepwet**, de Inlichtingenwet, de Aftapwet, de **WIV**, of weet ik veel hoe we het nieuwe afluisterreglement moeten noemen.

Als we het toch zo nodig over de privacy van de individuele burger willen hebben, sta mij dan óók even toe te wijzen op wat er in het China van Xi Jinping gaande is.

Oké, we mogen morgen net doen alsof we over het introduceren van die nieuwe wet meebeslissen. Wanneer we ons bij het stembureau vervoegen om in het kader van de gemeenteraadsverkiezingen het vakje achter de naam van Leefbaar Noordergat-vertegenwoordiger Baauwke Biggema rood te kleuren omdat hij net als wij van mening is dat de Hooivorksteeg voor tractorverkeer geopend moet blijven, kunnen we ons tegelijkertijd voor of tegen deze uitbreiding van de AIVD-bevoegdheden uitspreken. Zo onbegrijpelijk is het dus ook weer niet dat de media ons nu doodgooien met explicaties aangaande inhoud en consequenties van die wet. Ze willen dat we het snappen.

Ik snap het inmiddels en zal tegenstemmen, al besef ik donders goed dat koningin Kajsa mijn oordeel, indien het tot de meerderheid blijkt te behoren, achteloos terzijde zal schuiven: inspraak is zó 2017. Maar ik ben nu eenmaal een overtuigd aanhanger van de libertarische stelling dat de vrijheid van het individu, ondanks de maatschappelijke risico's die deze stelling met zich meebrengt, zo uitgebreid mogelijk dient te zijn. Om die reden maak ik toch gebruik van de mogelijkheid die mij morgen geboden wordt.

Ik wil echter tevens wijzen op de gang van zaken in China.

Daar ben je namelijk, als individu, helemáál de sjaak.

Ruben Terlou liet het al in een van de afleveringen van zijn prachtige documentaireserie Door het hart van China zien: de persoonlijke vrijheid van de Chinees wordt meer en meer ingeperkt. Zeker in de grote steden is het zelfs nagenoeg onmogelijk geworden onbespied te functioneren. Lang leve de digitale revolutie, maar niet heus: welke uitspraken je doet, wat je koopt, hoe je je in het verkeer gedraagt, met wie je zowel op de sociale media als op straat omgaat, noem maar op, werkelijk alle gegevens over je worden op last van de overheid verzameld en opgeslagen. Het zal uiteindelijk leiden tot een 'sociaal kredietsysteem', waarmee de almachtige staat de betrouwbaarheid van de burger meent te kunnen beoordelen. En aan de hand daarvan zal Xi Jinping, de man die zich onlangs tot president voor het leven liet benoemen, bijvoorbeeld gaan bepalen of jij al dan niet met de trein en/of het vliegtuig mag reizen.

Kan het enger?

„Een retourtje Sjanghai graag."

„Vergeet het maar, kameraad."

„Hoezo?"

„Je hebt op 12 juni 2019 je telefoonrekening een dag te laat betaald."

Het heropvoedingskamp is andermaal niet ver weg.

Laat ik voorlopig, als ik de wet waarover wij morgen iets mogen zeggen wil becommentariëren, dus maar niet naar Orwell's 1984 verwijzen.

In Peking kijkt Big Brother al veel nadrukkelijker toe.

In China ben je

helemáál de sjaak

**Cyriel Rosman – 17 maart 2018 - Als mensen ‘voor’ stemmen uit angst voor terreur, hebben wij het niet goed gedaan. – Algemeen Dagblad**

Marlou Gijzen zou het liefst haar stempas inlijsten en aan de muur hangen. ,,Maar dan kan ik niet stemmen." En Luca van der Kamp beseft waarschijnlijk woensdag pas, als hij in het stemhokje staat en met het rode potlood het 'tegen'-vakje inkleurt, dat het referendum echt is. ,,Het voelt nu nog zo onwerkelijk dat het allemaal gelukt is."

Dat 13 miljoen Nederlanders zich woensdag voor of tegen de nieuwe **Wet op de inlichtingen- en veiligheidsdiensten**, beter bekend als 'de **sleepwet**', mogen uitspreken, komt door Gijzen (23), Van der Kamp (22) en drie medestudenten. De wet is vorig jaar zomer al goedgekeurd door de Tweede en de Eerste Kamer en leek zonder veel reuring dit jaar in werking te treden. Totdat Gijzen zich boos maakte. ,,Er waren veel gerenommeerde instellingen en organisaties die kritiek hadden en toch ging-ie gewoon door. Dat vond ik echt heel raar." Van der Kamp: ,,Er staan dingen in die wet, waarvan wij denken: dat kán toch niet in Nederland."

Hun generatie leeft digitaal.

Uit peilingen blijkt dat jongeren vaker tegen de wet zijn dan ouderen. Van der Kamp: ,,Wat je online doet en communiceert, kan heel intiem zijn. Dát aftappen is echt heel anders dan alleen een telefoongesprek." Ze studeerden Informatica (Luca) en wiskunde (Marlou) en volgen nu beiden een master Logica. Van der Kamp: ,,Een studie waarbij je nadenkt over de mogelijkheden van systemen en complexe problemen." Precies de dingen waar de nieuwe wet over gaat.

**Steun**

Met drie anderen startten ze een handtekeningenactie om een referendum op te zetten. Ze kregen steun van Amnesty International, GeenStijl en Arjen Lubach. De vijf vroegen de redactie van Zondag met Lubach afgelopen najaar of ze aandacht wilde besteden aan hun campagne. Ze kregen een sms'je terug: ,,Kijk zondagavond even naar de tv." Een paar dagen na de '**sleepwet**'-uitzending waren de benodigde 300.000 handtekeningen binnen en was het referendum een feit. Van der Kamp, lachend: ,,Het is een beetje uit de hand gelopen."

Het was ook het moment dat de **Wiv** voor het grote publiek opeens in 'een **sleepwet**' veranderde. Een frame, zeggen voorstanders van de wet, het wekt de suggestie dat de geheime diensten straks niets anders doen dan data van (onschuldige) Nederlanders binnenharken. De AIVD vindt het een onjuiste voorstelling van zaken: grootschalig data aftappen mag alleen als het past in een onderzoeksopdracht en is onderhevig aan strikte controles.

Van der Kamp: ,,Dat deden we heel bewust. Het laat zien waar we tegen zijn en het geeft ook aan dat we niet tegen de hele wet zijn. Al zijn er wel steeds meer onderdelen bij gekomen waar we tegen zijn."

Gijzen: ,,Ik vind de informatie die de referendumcommissie geeft trouwens ook niet neutraal. Heb je gezien dat in hun brochure het rode potloodje veel dichter bij het vakje met 'voor' staat?"

Wat is jullie grootste bezwaar?

Van der Kamp: ,,Het sleepnet natuurlijk. Maar ik ben er ook van geschrokken dat de AIVD straks onschuldige mensen of organisaties mag hacken alleen maar om via hen toegang te kunnen krijgen tot mensen die wel verdacht zijn."

Gijzen: ,,De AIVD kan straks ook automatisch toegang krijgen tot allerlei databanken, van de overheid maar ook daarbuiten. Dat vind ik echt een belangrijk ding."

Bij de diensten zeggen ze dat het lastig discussiëren is met mensen die standaard uitgaan van de kwaadwillendheid van de geheime dienst.

Van der Kamp: ,,Ik geloof wel dat de AIVD ons land veilig wil maken. Maar het gaat erom wat zij onder deze wet allemaal zóu kunnen. Niet alleen nu, maar ook over een paar jaar."

Gijzen: ,,Als zij willen dat wij hen vertrouwen, moeten zij ons ook vertrouwen. En dat blijkt niet uit deze wet."

Jullie wilden mensen bewustmaken van deze wet en de gevaren ervan. Is dat gelukt?

Van der Kamp: ,,Nou, het gaat ook wel om de tegenstem hoor. Want er moeten echt veel dingen aan de wet veranderen. Met alleen de reparatiewet van GroenLinks ben je er nog niet."

Gijzen: ,,Als je naar de peilingen kijkt, wordt de uitslag spannend. Ik vind zelf: als mensen straks 'voor' de wet hebben gestemd uit angst voor terreur, dan hebben wij het niet goed uitgelegd. Want

veiligheid begint juist met privacy."

Dat u woensdag in het stemhokje 'voor' of 'tegen' de Wet op de inlichtingendiensten mag stemmen, komt doordat vijf studenten afgelopen zomer in opstand kwamen tegen de gevestigde politiek. ,,Het is een beetje uit de hand gelopen."

Wat je online doet, kan heel intiem zijn. Dát aftappen is echt heel anders.

**Marlou Gijzen 15 maart 2018 Als op zo'n manier grote groepen mensen worden doorzocht, zijn wij dan nog wel onschuldig totdat het tegendeel is bewezen?**

Hebben de inlichtingendiensten meer bevoegdheden nodig om terreuraanslagen te voorkomen of is de prijs daarvoor te hoog? De argumenten voor beide standpunten bij het raadgevende referendum van 21 maart. Het tegenargument komt van Marlou Gijzen, een van de initiatiefnemers van het referendum.
Beeld anp
Er zijn ontzettend veel geldstromen waarover een bank informatie heeft, bijvoorbeeld waar mensen pinnen en hoeveel. Wat nou als de AIVD deze data ook had? Voor een incidenteel onderzoek kan er weleens worden gevraagd naar wat van deze data. Maar om gedoe te voorkomen en wellicht om constant te kunnen controleren op mogelijke dreigingen, zou het beter uitkomen om automatisch gegevens van gebruikers te ontvangen, net zoals de bank zelf.
**Marlou Gijzen, een van de initiatiefnemers van het referendum, pleit tegen de wet.**Beeld RV
Dit mogen de veiligheidsdiensten binnenkort doen, met geautomatiseerde toegang tot databases van derden. Dit betekent dat de diensten real-time toegang krijgen tot een database, en nieuwe data binnenkrijgen precies wanneer de andere partij dat ook krijgt. Constant dus.

Deze toegang wordt verkregen via een informant. Deze moet vrijwillig de automatische gegevensverstrekking doorgeven. Maar wie durft er nou 'nee' te zeggen als iemand in de outfit van Plasterk zegt dat je in naam van de nationale veiligheid toegang tot de database moet verstrekken? En zelfs al zegt iemand 'nee', dan kunnen ze zo een volgend persoon proberen. Want wie deze toegang verschaft maakt niet uit. Het kan de baas zijn, de secretaresse, de systeembeheerder. Iedereen die toegang zou kunnen hebben tot de desbetreffende database.
En als deze toegang eenmaal is verschaft, is het onduidelijk hoe die weer kan worden stopgezet. De toestemming tot toegang blijft staan voor een jaar en kan worden verlengd. En omdat het niet geldt als bijzondere bevoegdheid, wordt hierop geen extra toezicht gehouden.

Als je deze databases dan ook nog combineert met andere data, zoals ov-chipkaardgegevens of data van telecommunicatiebedrijven en overheidsinstanties, heb je een gigantische hoeveelheid van verschillende soorten data, waaruit je allerlei patronen kan halen. Net als Google, Facebook en vele andere instanties lijkt het erop dat de AIVD gebruik wil gaan maken van Big Data. Grote groepen mensen monitoren was nog nooit zo makkelijk.

Er zijn risico's verbonden aan het gebruik van dit soort algoritmen. Profilering is er een van. Daarnaast zal het algoritme altijd fouten maken, en zullen er mensen die geen kwaad in de zin hebben onterecht worden aangewezen. Er zal niet alleen op basis van de uitkomsten van deze algoritmen worden gehandeld, zo staat het in de wet. Maar om erachter te komen of iemand nu wel of geen gevaar voor de samenleving is, is een grovere schending van privacy onontkoombaar. Daarnaast mogen gegevens die van belang zijn voor het opsporen van strafbare feiten worden gedeeld met het OM.
Waarom deze ingrijpende bevoegdheid nodig is, is onduidelijk, want met gerichte zoektochten leken de diensten het ook al prima te doen. Er zijn aanslagen voorkomen en de Russen werden gehackt. Toch komt er - naast het sleepnet, een dna-database en de mogelijkheid om derden te hacken - ook nog eens een automatische toegang tot databases mee in de nieuwe sleepwet. Waar het Verenigd Koninkrijk en Duitsland ook gebruikmaken van de bulkinterceptie, zijn wij de enige die deze DNA-database aanschaffen en de automatische toegang toestaan.

Als op zo'n manier grote groepen mensen worden doorzocht, zijn wij tegenwoordig dan nog wel onschuldig totdat het tegendeel is bewezen? Is dit recht niet van fundamenteel belang voor onze democratische rechtsstaat? Gelukkig kunnen we hier op 21 maart iets tegen doen.

**Lysanne van Schaik en Kevin Brongers** – 29 januari 2018 – Opinie: AIVD-succes maakt sleepwet overbodig.

Het was vorige week groot nieuws: de AIVD heeft de Amerikanen 'cruciale' informatie gegeven over Russische hackers na een eigen hackoperatie. Dat is fantastisch nieuws. Het verzamelen en delen van waardevolle informatie met bondgenoten is immers een kerntaak van de inlichtingendiensten. De Nederlandse inlichtingendiensten lijken ondanks het beperkte budget en de beperkte omvang prestaties van wereldklasse te kunnen leveren. Zo'n twee maanden vóór het referendum over een nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv), is het goed om te zien dat ook zonder de nieuwe wet de inlichtingendiensten uitmuntend werk kunnen leveren.

AIVD-baas Bertholee onthulde in College Tour dat zijn dienst in staat was meerdere grote aanslagen te voorkomen. De dienst kreeg toegang tot misschien wel de gevaarlijkste Russische hackersgroep. Premier Rutte gaf aan dat de nieuwe wet er 'sowieso moet komen'.

De laatste berichten tonen echter aan dat de inlichtingendiensten uitstekend in staat zijn waardevolle informatie te verzamelen met hun huidige bevoegdheden. De nieuwe Wiv is namelijk niet alleen een modernisering, maar ook een uitbreiding van aftapbevoegdheden. Alleen personen die worden verdacht van strafbare feiten mogen nu nog worden getapt. De nieuwe wet staat toe dat ook de gegevens van onschuldige personen in de omgeving van een verdachte mogen worden verzameld. Deze mogen dan maar liefst drie jaar worden bewaard.

## Grove privacyschending

De huidige Wet op de Inlichtingen- en Veiligheidsdiensten stamt uit 2002. Met de technologische ontwikkelingen van de laatste jaren is het natuurlijk tijd voor vernieuwing. De nieuwe wet is echter niet alleen een broodnodige update. Het mogen aftappen van informatie van mensen die niet verdacht worden van een strafbaar feit, en deze jarenlang bewaren, is een grove schending van het grondwettelijk beschermde recht op privacy.

Voor zulke ingrijpende inbreuken op grondrechten moeten zwaarwegende argumenten zijn. Daar is volgens ons geen sprake van. De nieuwe bevoegdheden garanderen grove privacyschending, maar het is niet bewezen dat ze effectief zijn. Niet alleen het recht op privacy komt in gevaar, maar ook de werkbaarheid. In de inlichtingenwereld geldt: 'hoe meer informatie, hoe meer werk.' Niet 'hoe meer informatie, hoe meer veiligheid'. De veiligheid kan juist in het geding komen door een onnodig grote berg aan informatie. De hooiberg wordt groter, de speld vinden alleen maar moeilijker.

## Meer geld en mankracht

We zijn niet gedwongen te kiezen tussen veiligheid en privacy, zoals Twan Huys stelde in een vraag aan Bertholee. De Jonge Democraten maken zich hard voor beide. Onze inlichtingendiensten hebben baat bij meer financiële middelen en mankracht. Uitbreiding van aftapbevoegdheden is onnodig. Daarom zijn wij voor sterke inlichtingendiensten, maar strijden voor een duidelijk 'nee' in aanloop naar het sleepwetreferendum. Wij hopen dat een nee-stem een krachtig signaal afgeeft aan onze regering dat Nederlanders goede inlichtingendiensten wensen die ons veilig houden, terwijl stevige waarborgen voor privacybescherming en toezicht zijn verankerd in de wet.

Een toezegging in het regeerakkoord is onvoldoende. Toekomstige bewindspersonen hoeven zich daar namelijk niets van aan te trekken. We strijden daarom voor een veilig Nederland beschermd door effectieve en slagkrachtige inlichtingendiensten, en tegen de nieuwe Wiv. De AIVD heeft geen extra bevoegdheden nodig om door te gaan met het goede werk dat ze al kunnen verrichten en hebben verricht.

**Marc Hijink – 20 maart 2018 – Het wordt 'Nee', die wet kan beter – NRC**

Wordt het Ja of Nee? Woensdag mogen we onze mening geven over de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (**Wiv**). De AIVD krijgt veel meer bevoegdheden om de kabel af te tappen en computers te hacken. We zullen nog jaren aan deze regels vast zitten; de vorige Wet op de inlichtingen- en veiligheidsdiensten dateert van zestien jaar geleden.

AIVD en MIVD hebben beter gereedschap nodig om ons te beschermen. Maar is dit het gereedschap dat we ze willen geven? Bladerend door het dossier op nrc.nl - 'Waarom zou je voor of tegen de Inlichtingenwet stemmen?' - en luisterend naar een paar uitstekende podcasts vind ik genoeg redenen om de wet bij te schaven. Ik deed met enige aarzeling ook nog de '**Wiv**-Test' van beveiligingsbedrijf Fox-IT (beantwoord alle zes vragen goed en je ziet: 'Fox-IT is altijd op zoek naar goed geïnformeerde mensen als jij'). Ook daar kom ik op 'Nee' uit.

Straks mogen veiligheidsdiensten ongericht data verzamelen, ook van mensen die geen doelwit zijn. ,,95 tot 98 procent" wordt meteen weggegooid, onder meer streaming video- en muziekdata. Het gaat om de 5 tot 2 procent die wel relevant is. Hoeveel daarvan weggegooid wordt is nog onduidelijk.

De afgetapte data kan drie jaar worden bewaard, veel langer dan de bewaarplicht die gold voor telecombedrijven. In die tijd kunnen gegevens gedeeld worden met buitenlandse overheden - ook data van burgers die geen doelwit zijn. Het gaat om metadata (wie heeft contact met wie en wanneer), maar inlichtingendiensten maken er geen geheim van dat ze de encryptie van WhatsApp willen kraken om mee te lezen.

De AIVD mag straks op jouw computer, je telefoon of de server van je provider inbreken om bij de gegevens van iemand anders te komen. Dat 'hacken via derden' klinkt geavanceerd maar het probleem is dat de hackmethoden van geheime diensten regelmatig uitlekken. Dat is een bedreiging voor iedereen, zoals we merkten met WannaCry.

Rob Bertholee, het hoofd van de AIVD, probeerde afgelopen weekend de gemoederen te bedaren. Hij vertelde bij WNL dat ,,Facebook meer van je weet dan wij". Internetdiensten waarvoor je je vrijwillig inschrijft kun je niet vergelijken met een overheid die dataverkeer aftapt. Toch is Facebook een goed voorbeeld: juist daar zie je hoe het mis kan gaan als dataverzameling onvoldoende gecontroleerd wordt.

Databedrijf Cambridge Analytica verwierf met een trucje 50 miljoen Facebookprofielen en destilleerde daaruit een blauwdruk voor politieke voorkeur. Daarmee kon het politieke sentiment in de VS en het Verenigd Koninkrijk gemanipuleerd worden. Data die bedoeld was voor Facebooks advertentiemachine, bleek eenvoudig te misbruiken voor andere doelen.

De **Wiv** wordt gepresenteerd als een methode om aanslagen te voorkomen en de veiligheid van Nederlanders bij buitenlandse missies te vergroten. Dat is nu het doel. Zou dat over zestien jaar nog het geval zijn? Of hebben we onszelf in 2034 opgescheept met een regering die haar burgers controleert - bijvoorbeeld op religie of achtergrond - in plaats van beschermt? Die potentiële *function creep* moet uitgesloten worden. Dus nee - die wet kan beter.

**Financieel Dagblad: Ineffectiviteit van Sleepwet is de laatste strohalm voor de tegenstanders**

Bernold Nieuwesteeg

Bij de meeste privacy-activisten (en andere liefhebbers van een niet al te overheersende overheid) dringt het besef door: het tegenhouden van de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv), bijgenaamd de **sleepwet**, is vechten tegen de bierkaai. De coalitie legt een eventuele nee-stem bij het referendum al bij voorbaat naast zich neer. Zo stelde CDA-leider Sybrand Buma dat hij wil dat de **sleepwet** doorgaat en dat het referendum niet als een echt referendum gezien moet worden. De slag lijkt dus bij voorbaat al verloren. Hoe kunnen we de oorlog winnen en de **sleepwet** alsnog van tafel krijgen?

Er is nog een smal pad door de bergen. Bij een nee-stem moeten we afdwingen dat we gaan meten of de wet daadwerkelijk leidt tot minder terrorisme. We moeten het frame veranderen van zorgen over 'Big Brother' naar zorgen over effectiviteit. Dan zal blijken wat velen nu al vermoeden, maar weinigen binnen de coalitie willen geloven: een **sleepwet** werkt niet.

Waarom werkt een sleepnet niet? Problematisch bij de zoektocht naar terroristen is dat het er heel erg weinig zijn. Een paar terroristen te spotten tussen miljoenen mensen is dus heel lastig. De bekende speld in de hooiberg. Het sleepnet verzamelt miljoenen datapunten van smartphones, televisies en laptops in duizenden huizen, buurten en wijken. Meer hooi op de hooiberg dus.

Maar is er dan niet een slimme data-analysetechniek om verdachte patronen uit die miljoenen datapunten te destilleren? Het klopt dat er de afgelopen jaren enorme vooruitgang is geboekt op het gebied van het analyseren van grote hoeveelheden data. Maar een analyse van big data levert eerder een ruwe schets op dan een precies schilderij. Het is moeilijk, zo niet onmogelijk, de analyse zo te doen dat we precies de terroristen eruit filteren. De waarschuwingssystemen zullen overspoeld worden met onschuldige verdachten. Op zijn best kunnen we nu een speld gaan zoeken in een nieuwe hooiberg die even groot is als de hooiberg waar we aanvankelijk mee zaten in het oude systeem.

We schieten dus niet zoveel op met de nieuwe wet, maar daar hoor je nu weinig mensen over. Het is merkwaardig dat de discussie over de doelmatigheid is ondergesneeuwd in het publieke debat. En dat terwijl de ineffectiviteit van de wet juist voor de tegenstanders de laatste strohalm lijkt te zijn om de wet alsnog af te schieten, zij het in een later stadium.

Hoe heeft het zo ver kunnen komen? Aanvankelijk leken de tegenstanders het goede mediaframe te hebben door de Wet op de inlichtingen- en veiligheidsdiensten om te dopen tot **sleepwet**. Deze term geeft treffend weer dat er op grote schaal data verzameld worden en dat de privacy van burgers in gevaar is. Maar schijn bedriegt: het zijn juist de voorstanders van de **sleepwet** die deze slim in de markt hebben gezet. Namelijk exact als een keuze tussen meer veiligheid en het verlies van een beetje privacy (je zou zelfs kunnen beargumenteren dat de term **sleepwet** daarbij heeft geholpen). We weten dat in tijde van terrorisme de meerderheid van de Nederlanders op safe speelt. Sterker nog, uit wetenschappelijk onderzoek blijkt dat mensen er helemaal niet goed in zijn de waarde van hun privacy in te schatten. We verkopen bijvoorbeeld onze data aan Facebook en Google voor een vaak belachelijk lage prijs.

Wellicht kunnen tegenstanders van de wet de Nederlander raken op een plek waar zeker een nationale gevoeligheid zit: de portemonnee. Als blijkt dat miljoenen aan belastinggeld gespendeerd worden aan een wet die de pakkans op terroristen niet vergroot, dan zouden de rapen gaar moeten zijn.

De uitslag van het referendum wordt genegeerd, dat weten we nu al. Maar als een grote meerderheid 'nee' stemt, moeten we gaan meten of de wet leidt tot het vangen van meer terroristen. Denk bijvoorbeeld aan een vergelijking met andere landen of de periode van voor de **sleepwet**.

Nu wordt er louter geëvalueerd of de **sleepwet** wel genoeg privacybescherming biedt. Precies dus de uitruil tussen veiligheid en privacy waar we van weg willen.

**Jaap-Henk Hoepman: Tegen tegen de Sleepwet! Het Financieele Dagblad, 26 augustus 2017**

Op 11 juli 2017 nam de Eerste Kamer de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv) met een meerderheid van stemmen aan. In die wet krijgen de AIVD en de MIVD nieuwe bevoegdheden. Als de wet op 1 januari 2018 in werking treedt, krijgen deze veiligheidsdiensten de mogelijkheid ook 'kabelgebonden' communicatie (lees: internetverkeer) ongericht te onderscheppen. Ook kunnen ze, rechtstreeks, toegang krijgen tot gegevensbestanden van andere organisaties en bedrijven. En mogen ze de verkregen gegevens delen met buitenlandse inlichtingendiensten.

Niets meer aan te doen, zou je zeggen. Toch niet. Eerder al meldden twaalf organisaties, waaronder burgerrechtenorganisatie Privacy First en de Nederlandse Vereniging van Strafrechtadvocaten, dat ze naar de rechter zullen stappen om deze '**sleepwet**' ongeldig te laten verklaren. En onlangs verzamelde een groepje Amsterdamse studenten in een week 10.000 handtekeningen voor een initiatief om een raadgevend referendum over de **Sleepwet** te houden.

Vanwaar deze acties? Het is toch niet vreemd om onze inlichtingendiensten de macht te geven om internet in de gaten te houden? Het gros van de communicatie, van gewone burgers, maar ook van criminelen en terroristen, vindt immers daar plaats?

Dat klopt. Ik zal hier niet een discussie beginnen over de vraag of we überhaupt nog geheime diensten nodig hebben in deze tijd van radicale transparantie. Maar er zijn een aantal dingen grondig mis met deze wet.

De wet Wiv wordt niet voor niets '**sleepwet**' genoemd. De inlichtingendiensten mogen met een groot en wijd sleepnet data op internet verzamelen. Daarmee worden bij het zoeken naar terreurverdachten ook veel data van onschuldige burgers verzameld en geanalyseerd.

Dit is de wereld op zijn kop. Dat een paar onschuldige burgers bijvangst zijn in de jacht op terroristen is te billijken. Maar nu lijkt het erop alsof de terroristen een toevallige bijvangst zijn in de zee van data van onschuldige burgers. Die overvloed aan ongeanalyseerde data mag ook nog eens met al dan niet bevriende geheime diensten van andere landen gedeeld worden. Data van onschuldige burgers komen zo in de handen van een andere overheid terecht. Net zoals een sleepnet ecologische schade toebrengt, heeft deze **sleepwet** maatschappelijke (privacy)schade tot gevolg.

Ook ons Privacy & Identity Lab op de Radboud Universiteit Nijmegen (RU) voerde vorig jaar een 'privacy impact'-assessment uit op het wetsvoorstel. Naast de hierboven genoemde bezwaren vinden wij dat de wet dwingender 'privacy by design' zou moeten opleggen. De 'drietrapsraket' van verzamelen, selecteren en analyseren zou technisch zo ingericht moeten worden dat privacyrisico's en misbruik beperkt worden. Ook houdt de wet onvoldoende rekening met belangrijke toekomstige technologische ontwikkelingen zoals drones, geavanceerde data-analyse gecombineerd met nieuwe observatiemiddelen en de data-overvloed die wordt veroorzaakt door het Internet der Dingen. Daarmee worden de privacyrisico's van voorgestelde bevoegdheden onderschat.

Zoals Hans de Zwart van Bits of Freedom onlangs zei: 'Het wordt binnen een paar jaar voor de overheid opeens technisch mogelijk én - niet onbelangrijk - betaalbaar om iedereen altijd 100% in de gaten te houden.'

Met als gevolg dat we ons gaan gedragen alsof er ieder moment van de dag een politieagent met ons meekijkt. Onlangs vroeg het Department of Justice in de VS de gegevens van 1,3 miljoen bezoekers van een anti-Trumpwebsite op. Hoe vrij voel je je dan nog om je kritisch te uiten over Donald Trump? En hoe zeker zijn we dat zoiets niet in Nederland gebeurt?

Als laatste: veel is al gezegd over het gebrekkige toezicht op de veiligheidsdiensten. Maar ook de politiek laat het afweten. De commissie 'stiekem' heeft slechts vijf leden, waarvan er vier lid zijn van onze toekomstige regering. De commissie telt straks dus slechts één oppositielid!

Met andere woorden: dit moet echt anders. Om echt een referendum af te dwingen hebben de studenten uit Amsterdam 300.000 handtekeningen nodig. Tekenen dus!

**Maurits Martijn – 20 maart 2018 – Waarom ik tegen de nieuwe wet voor de geheime diensten stem – De Correspondent**

Wat ga je stemmen tijdens het referendum?

Het is me de afgelopen weken vaak gevraagd, door collega's, vrienden en debat-organisatoren. Ik ben er definitief uit. Vorige week analyseerde *Sleepwet? Vier cruciale inzichten over de wet voor de geheime diensten*ik een aantal cruciale punten uit de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv). Nu geef ik drie redenen waarom ik woensdag tegen stem tijdens het referendum.

Dit gesprek moeten wij continu blijven voeren

Ik schrijf nu een paar jaar over de diensten en begin hun werk steeds beter te begrijpen. Door veel met mensen uit het veld te spreken en me te verdiepen in het feitelijke werk van de diensten besef ik: ons beeld van de diensten is vertekend.

Ja, dat werk is op zijn tijd ijzingwekkend spannend. James Bond, Jason Bourne, dat werk. Zoals de operatie tegen de Russische hackers waar *de Volkskrant* en *Nieuwsuur* in januari meeslepend over berichtten. Of de heimelijke afluisteroperaties in 'rode' ambassades tijdens de Koude Oorlog, die ik met Cees Wiebes onthulde .
En ja, er staat ook écht iets op het spel. Soms doet de informatie die de diensten verzamelen ertoe, op - laten we zeggen - *Homeland*-niveau. Denk aan bijdragen aan het onderzoek van speciale aanklager Robert Mueller naar de Russische banden van team-Trump. Aan cruciale informatie over Talibanstrijders tijdens de oorlog in Afghanistan. Aan data die naar Somalische piraten leidden .
Veel vaker nog heeft het werk van de diensten niets te maken met wat historicus Constant Hijzen 'op hol geslagen publieke fantasieën' noemt over totalitaire sleepnetten, de gedachtepolitie of de 'deep state'.
Dan zitten de medewerkers van de diensten gewoon van negen tot vijf achter hun bureau. Dan schrijven ze rapporten, vergaderen ze uren achter elkaar, drinken ze automaatkoffie. Dan is die man met beige broek en bruine brogues die zijn bammetjes eet in de trein niet de doorsnee ambtenaar waar je hem voor aanziet, maar een AIVD'er op weg naar de zaak.

Inbreuk maken op de grondwet kun je wel zien als de essentie van het inlichtingenwerk, met de staatsveiligheid als hoger doel

Ons beeld van de diensten mag troebel zijn, de praktijk weerbarstig (en saaier), kraakhelder is dat in theorie (bij wet) de diensten ongelooflijk veel mogen - nu en straks nog meer. Ze hebben geen *license to kill*, maar kunnen wel strafbare feiten plegen en op grote schaal burgerrechten schenden. Inbreuk maken op de Grondwet kun je zien als de essentie van het inlichtingenwerk, met de staatsveiligheid als hoger doel.
Nu zijn sterke diensten met dito bevoegdheden goed te verantwoorden in een tijd van terroristische aanslagen in alle buurlanden, serieuze digitale gevaren, een hernieuwde nucleaire wapenwedloop en driftige leiders aan de macht in China, de Verenigde Staten, Turkije en Rusland.

Dan gaat het dus erom de juiste balans te vinden. Een balans tussen de reële gevaren en de indringende bevoegdheden die nodig zijn die te bestrijden. Een afweging tussen wat nodig en gewenst is aan de ene kant en wat er gebeurt en kan gebeuren aan de andere kant, tussen wat *nice to know* is en *need to know* zou moeten zijn.
En die afweging wordt ook gemaakt, bij de diensten, door de ministers, de toezichthouders én in de wet zelf. Maar het gesprek hierover moet óók in de openbaarheid plaatsvinden. Juist in de openbaarheid. Waartoe zijn de diensten op aarde? Wat doen ze? Wat mogen ze? Wat staan we hun toe?

Begrijp mij niet verkeerd: ik pleit hier niet voor totale transparantie. Geheime diensten heten geheime diensten met een reden. De staatsveiligheid verdedig je niet als iedereen mee mag kijken. Maar de beruchte 'geheimhoudingskramp' waar de diensten in Nederland aan lijden, is het andere uiterste.

De afgelopen weken hebben we gezien dat het ook anders kan. We spraken wekenlang over nota bene een *wet*, over veiligheid en privacy, over noodzakelijke geheimhouding en minimale transparantie. Natuurlijk, iedereen stond in campagnestand, beide kampen hebben aardig wat demagogie laten horen, niet iedereen had de feiten op een rij en sommige campagnestrategieën leverden meer irritatie dan informatie op.
Maar er was een gesprek gaande. Een wezenlijk gesprek. Cruciaal voor de legitimiteit van de diensten. Voor de democratische inbedding. Voor de veiligheid én de vrijheid. En tegen het op hol slaan van publieke fantasieën.

Dit zou een permanent gesprek moeten zijn, dit tik je niet even af met een referendum. AIVD-baas Rob Bertholee zou niet alleen in campagnetijd moeten aanschuiven bij *De Wereld Draait Door* en WNL , maar een graag geziene gast moeten blijven in media en talkshows. Of anders geformuleerd: eigenlijk zou Rob Bertholee doorlopend in campagnestand moeten staan om het werk van de diensten te verkopen en de noodzaak en relevantie ervan te verdedigen.
**Mijn eerste reden om tegen te stemmen is daarom een strategische:** ik hoop dat een massaal nee een signaal is dat het kabinet en de diensten doet beseffen dat de burger wil weten wat de AIVD en MIVD doen, waarom ze het doen en met hen in gesprek wil blijven.
Bij een vóór-stem woensdag is het risico groot dat de diensten denken 'klus geklaard' en terug in hun oester kruipen om daar voorlopig niet meer uit te komen. Een tegenstem kan ervoor zorgen dat de publieke en journalistieke aandacht voor de diensten blijvend is. Het kabinet hoeft de wet niet aan te passen als een grote meerderheid tegen de wet blijkt te zijn, maar kan die uitkomst ook moeilijk negeren.

## Het toezicht en de waarborgen zijn wiebelig en dat kan beter

Voorstanders van de wet pochen dat het Nederlandse toezichtssysteem op de diensten tot de top behoort. 'Geen dienst ter wereld wordt zo op de vingers gekeken als bij ons de AIVD en MIVD', *Lees hier het interview met Paul Abels.*zei bijzonder hoogleraar Governance of Intelligence and Security Services én oud-AIVD'er Paul Abels. 'Ik ben ervan overtuigd dat wij de best gecontroleerde dienst, in elk geval in Europa, waarschijnlijk in de wereld, zijn', aldus directeur-generaal AIVD Rob Bertholee. Onduidelijk is of zij een punt hebben: *NRC* concludeerde al eens dat deze stelling niet te checken *NRC factcheckte deze uitspraak en concludeert: niet te checken.*is. Maar ook al hebben ze gelijk, dan nog zegt dit bar weinig. *Goed toezicht op papier, betekent niet per se goed toezicht in de praktijk*. Waar iedereen het wel over eens is: bij de nieuwe vergaande bevoegdheden van de diensten horen even sterke waarborgen en toezicht.
Laat ik beginnen met het goede nieuws: de controle is in de nieuwe wet beter geregeld dan in de vorige. Kort gezegd, er komt een nieuwe toezichthouder, de Toetsingscommissie Inzet Bevoegdheden (TIB), die elke keer dat de diensten gebruik willen maken van hun bijzondere bevoegdheid, zoals het grootschalig verzamelen van kabelcommunicatie, toetst of dit wel mag. Deze toets is bindend: zegt de commissie nee, dan gebeurt het niet.

## Goed toezicht hebben op papier, betekent niet per se goed toezicht in de praktijk

Ook nieuw: als de diensten een advocaat of journalist willen aftappen of hacken, hebben zij toestemming nodig van een rechter. Verder wordt de rol van de bestaande toezichthouder, de Commissie van Toezicht op de Inlichtingen-en Veiligheidsdientsen (CTIVD), uitgebreid; de commissie krijgt een nieuwe afdeling voor klachten die over de AIVD of MIVD zijn geuit.

Dit is een hele vooruitgang. En een die voldoet aan het Europees Verdrag voor de Rechten van de Mens. In theorie dan. *Want ondanks alle mooie verhalen van de voorstanders, is fundamentele kritiek mogelijk op de uitwerking van het toezicht en andere waarborgen in de wet.*

En die kritiek is ook geleverd *Lees hier meer over de fundamentele kritiek op het toezicht*. Door gerespecteerde kenners van de rechtsstaat als de onafhankelijke Raad van State en Raad voor de Rechtspraak , door enkele van de best ingevoerde juristen, als Axel Arnbak en Dorien Verhulst, en door toezichthouder CTIVD zelf.
Die kritiek gaat voor een belangrijk deel over de nieuwe toezichthouder, de TIB, die straks uit drie personen zal bestaan. De Raad van State voorziet een versnipperd en gefragmenteerd systeem met de TIB en CTIVD naast elkaar, wat de kwaliteit van het toezicht bedreigt.

De nieuwe TIB krijgt daarbij geen toegang tot de computersystemen van de diensten, De Raad van State heeft daardoor *'ernstige twijfels' of het toezicht 'effectief bescherming [kan] bieden aan de grondrechten van burgers'*.

Sterker, zij verwacht dat de toets van een TIB nagenoeg altijd positief zal uitvallen: zeg maar eens 'nee' tegen een verzoek als je de praktijk niet kent, maar mogelijk wél een verkeerd besluit kunt nemen, met alle gevolgen van dien.

Alibi-functie van de TIB

De TIB zal daarom een 'alibi-functie' vervullen, denkt de Raad. Een stempelmachine, met haast altijd een positief oordeel. Zijn advies: schrijf die hele TIB uit het wetsvoorstel en leg de taken ervan bij de bestaande CTIVD.

Het kabinet en de diensten daarentegen pronken met de TIB - al is een vorm van bindend toezicht vooraf pas de wet ingefietst na een storm van kritiek - en benadrukken het onafhankelijke karakter van die commissie. Maar ook daar zijn vraagtekens bij te zetten.

Want tot veler verrassing neemt Ronald Prins *Dit profiel schreef ik in 2011 over Ronald Prins*plaats in de TIB, naast twee oud-rechters. Prins was tot 1 januari 2018 directeur van Fox-IT, een bekend Nederlands beveiligingsbedrijf dat nauw samenwerkte met de diensten en andere takken van de overheid, en heeft zich in de media gepresenteerd als uitgesproken voorstander van de nieuwe wet. Straks moet hij de inzet van die nieuwe bevoegdheden toetsen op rechtmatigheid. Hij heeft daarvoor zeker de expertise in huis. Maar kan hij genoeg afstand bewaren? Hoe onafhankelijk kan iemand oordelen die zelf bij de AIVD heeft gewerkt en wiens bedrijf technologie leverde aan de diensten?

## Ondanks al die tegenwerpingen noemt de CTIVD de nieuwe wet weliswaar 'niet volmaakt' maar toch 'in balans'

Er zijn veel meer vragen. Zo is er geen *bindend* toezicht tijdens de verwerking van al die bakken data, hoewel onder andere de Nationale Ombudsman en de CTIVD daarop hebben aangedrongen. Als operaties onrechtmatig burgerrechten schenden worden ze dus niet vanzelfsprekend stopgezet.*Lees hier bijvoorbeeld de analyse van het Institute of Information Law.*
Ook is nog onduidelijk hoe het toezicht zal plaatsvinden op de verwerking door de diensten van al die bakken data. Welke algoritmes worden daarop losgelaten? En hoe wordt dit gecontroleerd? *Hier kun je meer over lezen in deze interessante bijdrage van een medewerker van de CTIVD.*Ander heikel punt is de uitwisseling van ruwe bulkgegevens met buitenlandse inlichtingen- en veiligheidsdiensten. Daarvoor is tot verbazing van critici juist geen toestemming nodig van de toezichthouder.
Ondanks al die tegenwerpingen noemt *Dat doet de CTIVD in de eindbalans*de CTIVD de nieuwe wet weliswaar 'niet volmaakt' maar toch 'in balans'. Wel benadrukt ze dat die balans er pas is gekomen door de vele 'moties, toelichtingen en (...) toezeggingen' die in de loop van het wetstraject zijn toegevoegd. Zoals de toezeggingen door het kabinet dat de wet na twee jaar wordt geëvalueerd en dat

‘van het willekeurig en massaal verzamelen van persoonsgegevens geen sprake kan, mag en zal zijn’. Deze cruciale waarborgen staan niet in de wet zelf.
**Voor mij is dit de tweede reden om tegen te stemmen. Een volmaakte wet bestaat niet, maar een stevigere en toekomstbestendiger wet is mogelijk.** Ik vind het onbegrijpelijk dat het kabinet essentiële kritiek van deskundige organisaties als de Raad van State en de Raad voor de Rechtspraak negeerde. De diensten mogen rechten van burgers schenden en burgers verdienen de hoogst mogelijke bescherming. Is het niet voor nu, dan toch zeker wel voor de toekomst. ‘Wettelijke waarborgen zijn er voor als het misgaat’, vertelde de CTIVD-voorzitter Harm Brouwer mij ooit. ‘Als er, bijvoorbeeld, een politiek klimaat ontstaat waarbinnen onafhankelijk toezicht maar lastig wordt gevonden.’

Een tegenstem als signaal aan het parlement: pak de Commissie Stiekem aan

Over die andere vorm van toezicht is al decennia gedoe: de controle van de diensten door de Tweede Kamer. Dat gebeurt in speciale commissies, debatten en in de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD), beter bekend als de Commissie Stiekem, waar de fractievoorzitters van de vijf grootste partijen uit de Tweede Kamer in zitten.

Onderzoekers wijzen consequent op het gebrekkige niveau van deze parlementaire controle. Parlementariërs hebben weinig kaas gegeten van het werk van de diensten - uitzonderingen daargelaten - en dat zie je terug in de debatten.

De Commissie Stiekem is een apart verhaal. In de woorden van inlichtingenexpert Cees Wiebes : de Commissie Stiekem had beter de Commissie Afwezig kunnen heten. Onder fractievoorzitters is de commissie niet populair *Dit schreef ik eerder over die commissie*. Zo was in 2016 gemiddeld maar 54 procent van hen aanwezig bij vergaderingen van de Commissie Stiekem. Dat is te weinig, in een jaar van bloedige aanslagen, coups en revoluties.
Je kunt je ook afvragen of de fractievoorzitters - bij uitstek generalisten en geen specialisten - wel op hun plek zijn als dé controleurs van de diensten. Nee, zegt bijvoorbeeld oud-fractievoorzitter Femke Halsema, die jaren in de Commissie zat. Haar analyse: de behoefte van een partij aan aandacht in de media is zo groot, dat fractievoorzitters zich liever op een ander terrein profileren.

Toen Dijkhoff nog Kamerlid was, was hij uitzonderlijk goed geïnformeerd over de diensten

Anders komen ze ‘in een rechtsstatelijke niche terecht’, en vrezen ze dat journalisten hen ‘nooit meer zullen benaderen voor de zorg bijvoorbeeld, of sociale zekerheid’. ‘Dus dat zijn allemaal afwegingen die fractievoorzitters maken en die haaks staan op hele grondige en goeie controle van de AIVD’, zei Halsema tijdens een bijeenkomst over de AIVD.
Dit wordt breed erkend, ook door oud-minister van Binnenlandse Zaken Johan Remkes, die van 2002 tot en met 2007 politiek verantwoordelijk was voor de AIVD. In de Commisie Stiekem ‘werd destijds nauwelijks doorgevraagd door de fractievoorzitters’ , zei Remkes.
**Mijn derde reden om tegen te stemmen is als aansporing voor de Tweede Kamer om hun taak nu eens serieus te nemen.** Om meer werk te maken van de Kamercommissies en plenaire debatten. Een massaal ‘nee geeft parlementariërs een signaal: het volk vindt dit belangrijk. Voor de duidelijkheid: het parlement bepaalt zelf hoe het de diensten controleert. Daar heeft de Wiv niets over te zeggen. Een aanpassing van de Commissie Stiekem moet dus ook uit de Kamer zelf komen.
Die vroeg de regering vorig jaar al te onderzoeken hoe in andere landen het parlement de diensten controleert, in de hoop op goede ideeën om de Nederlandse praktijk te verbeteren. Een meerderheid die tegenstemt en een hoge opkomst zet hopelijk vaart achter die plannen. De tijd vraagt erom.

Interessant genoeg is VVD’er Klaas Dijkhoff, als fractievoorzitter van de grootste partij, voorzitter van de Commissie Stiekem. Toen Dijkhoff nog gewoon Kamerlid was, was hij niet alleen uitzonderlijk

goed geïnformeerd over de diensten, hij had ook zeer uitgesproken ideeën over nieuwe en betere vormen van parlementaire controle *Lees hier meer over de plannen van Dijkhoff*.
Sinds Dijkhoff in het centrum van de macht zetelt, weigert hij zich hierover uit te spreken. Wellicht haalt een oorverdovend nee hem uit die stilteretraite.

Vóór het debat en daarom tegen

Het is al vaak gezegd: *Rob Wijnberg zegt het ook*: een referendum kan geen recht doen aan deze ingewikkelde wet. Want wat wijs je af als je tegen stemt? Wat krijg je ervoor terug? En als je 'ja' zegt, ben je dan overal vóór? Voor het hacken van derden én het zogeheten sleepnet? En vind je dan automatisch dat het toezicht perfect geregeld is? Lastig.
Toch heeft dit referendum nu al zijn waarde bewezen. Voor het eerst vindt er een echt wezenlijk debat plaats over de macht van de geheime diensten. Ik ben vóór dit debat. Daarom stem ik tegen.

**Rob Wijnberg – 20 maart 2018 - Waarom de zucht naar méér inlichtingen nooit zal ophouden (en ik dus 'tegen' stem bij het referendum) – De Correspondent**

Toen ik collega-journalist Joris Luyendijk een tijdje geleden een vraag voorlegde waar ik al weken mijn hoofd over brak, antwoordde hij met een briljante wedervraag: 'Is het een puzzel of een mysterie?'

Gevraagd naar het verschil zei hij: 'Een puzzel is een vraag waar je het antwoord niet op weet, omdat de onderdelen van het antwoord niet op de juiste plek liggen. Een mysterie is een vraag waarop je het antwoord niet weet omdat je de vraag niet begrijpt.'

Daar moest ik aan denken toen ik me afvroeg wat ik ging stemmen tijdens het referendum over de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) 2017 - onder critici beter bekend als de 'sleepwet'.

Want hoewel voorgespiegeld als een puzzel met drie mogelijke antwoorden (ja, nee of blanco), is het referendum natuurlijk meer een mysterie: waar stem je eigenlijk over?

De vraag die voorligt, is op allerlei manieren volstrekt onduidelijk. Wordt de wet bijvoorbeeld afgeblazen als er massaal 'nee' wordt gestemd? CDA-leider Sybrand Buma heeft alvast gezegd van niet. Is een opkomst van 30 procent genoeg om het referendum serieus te nemen? En zo ja, wordt de wet bij een 'nee' dan aangepast? Hoe dan?

Als je tegen het verzamelen van data over alle burgers bent, maar meer hackbevoegdheid op basis van reëele verdenkingen wel een goed idee vindt, wat dan? En als er een ‘ja’ komt, waar is er dan eigenlijk ‘ja’ tegen gezegd? Meer veiligheid? Wat voor veiligheid? Is een land waarin de overheid alle burgers online kan volgen en hacken veiliger? Is privacy zelf niet een vorm van veiligheid?

Een mysterie dus.

Het cruciale verschil tussen known unknowns en unknown unknowns

De ironie is dat niet alleen het referendum zélf meer een mysterie dan een puzzel is: het inlichtingenwerk waar deze wet om draait drijft op precies datzelfde verschil. Sterker nog, het verschil tussen puzzel en mysterie komt uit de inlichtingenwereld - en onderscheidt zich juist op dit punt van politiewerk.

Politiewerk (bijvoorbeeld: wie heeft deze diefstal gepleegd?) is een kwestie van puzzelen: je weet de vraag en het antwoord is een kwestie van de juiste stukjes op de juiste plek krijgen. Puzzels zijn op te lossen door het vergaren van meer (en juiste) informatie.

Inlichtingen (bijvoorbeeld: wie gaat een aanslag plegen?) draaien daarentegen om mysteries: er is een dusdanige mate van onzekerheid dat het fundamenteel onduidelijk is wat eigenlijk is waar je naar op zoek bent.

Anders gezegd: puzzels draaien om known unknowns - mysteries om unknown unknowns.

Hier vind je de beroemde persconferentie terug waar de toenmalige Amerikaase minister van Defensie Donald Rumsfeld spreekt over ‘unknown unknowns’.

Dat is een cruciaal onderscheid om in gedachten te houden bij dit debat - en bij je afweging of je voor of tegen de Wiv 2017 bent. Want: omdat inlichtingen draaien om het voorspellen en inschatten van unknown unknowns, is er geen natuurlijke grens aan de hoeveelheid informatie die je zou kunnen en moeten verzamelen om, bijvoorbeeld, terroristische aanslagen te voorkomen. Simpeler gezegd: voor het oplossen van mysteries kun je nooit genoeg weten.

De essentie van de sleepwet: doen alsof inlichtingenwerk een puzzel is

Voorstanders van de wet suggereren een andere werkelijkheid. Zij spiegelen de aard van inlichtingen als puzzel voor. De essentie van bijna al hun argumenten voor de sleepwet komt hier op neer: als de AIVD en MIVD simpelweg meer data kunnen verzamelen, kunnen zij dreigingen en risico’s beter voorspellen en daarmee onze veiligheid vergroten.

Zij schermen daarbij met redenaties als die van VVD-prominent Arthur Docters van Leeuwen, die stelt dat er zonder deze wet ‘meer aanslagen’ zullen zijn. Dat argument is problematisch, omdat het onweerlegbaar is. Niet omdat er geen causaal verband kan zijn tussen inlichtingen en het voorspellen van dreigingen als aanslagen, maar omdat het omgekeerde evengoed waar is: er is geen moment waarop de inlichtingendiensten ‘genoeg’ weten en er dus géén aanslagen meer zullen komen.

Anders gezegd: voor een antwoord op de vraag ‘Wie van de zeven miljard zielen op aarde is de volgende die met een bomgordel een bus in loopt?’ is nooit genoeg informatie voorhanden. De sleepwet is daarmee, de facto, een wet zonder eind: waar stopt de behoefte aan nóg meer bevoegdheden voor het verzamelen van data over burgers?

De morele vraag: hoe gaan we als samenleving om met risico’s?

Het enige mogelijke antwoord daarop is van morele aard: een politieke inschatting van hoe (on)acceptabel wij als samenleving de risico’s vinden waar inlichtingen- en veiligheidsdiensten ons voor moeten behoeden.

Zelf behoor ik tot de school die stelt dat we niet de illusie moeten kweken dat risico's zoals terrorisme puzzels zijn. Want dat opent de deur naar een totalitaire staat, die alles wil weten van iedereen. Er is dan geen enkel argument meer voorhanden om van het 'sleepnet' in de Wiv 2017 niet uiteindelijk een alomtegenwoordige Big Brother te maken. Je wilt toch geen toekomstig bloed aan je handen hebben?

Natuurlijk, ook inlichtingen- en veiligheidsdiensten moeten meegaan met hun tijd. In het digitale tijdperk is een krant met een gaatje erin, van waarachter de spion de vijand in de gaten kan houden, niet genoeg. Niemand betwist de noodzaak van gerichte bevoegdheden om ook in de 21ste eeuw bruikbare inlichtingen te kunnen vergaren.

Maar, de vraag is niet alleen in wat voor tijd we leven, de vraag is ook in wat voor tijd we willen leven. Een tijd waarin we stapje voor stapje onze grondrechten, privacy en vrijheid willen opgeven voor de illusie van controle over bedreigingen die uiteindelijk nooit beheersbaar zullen zijn? Of een tijd waarin we begrijpen dat veiligheid uiteindelijk als doel heeft juist die grondrechten, privacy en vrijheid, te waarborgen? Ik stem voor dat laatste.

En daarom stem ik 'tegen' tijdens het referendum.

**Adriana Rumulova, Anouk Ruhaak, Saskia Naafs – 15 maart 2018 - Een nog grotere hooiberg bouwen boven op een speld; Onderzoek De nadelige gevolgen van de 'sleepwet' – De Groene Amsterdammer**

Volgens de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten, waarover 21 maart een referendum is, mogen inlichtingendiensten onbeperkt gegevens binnenhalen van onverdachte burgers. Dat leidt niet tot meer veiligheid. Wel tot meer onvrijheid.

**'WOW, WAT GEBEURT HIER?** Ik heb toch niks verkeerd gedaan?' Ibrahim (Abe) Mashal staat ingeklemd tussen wel twintig vliegveldbeveiligers. Het is een woensdagmiddag in april 2010 en Mashal, een ex-marinier en vader van drie kinderen, is op het vliegveld van Chicago om in te checken voor zijn vlucht naar Spokane. Hij moet daar een hondentraining geven.

De grondstewardess die met zijn rijbewijs verdween komt terug en zegt dat hij op de *no fly list* staat van het Terrorist Screening Center, een internationale lijst met zo'n 64.000 bekende of vermoede terroristen. Een reden voor zijn vliegverbod krijgt hij niet, maar als Mashal thuiskomt wachten twee fbi-agenten hem op. Ze willen alles weten over zijn Palestijnse vader, zijn buitenlandse kennissen en of hij bij de marine bommen heeft leren maken. Ook Mashals klant in Spokane krijgt bezoek van de fbi en zegt vervolgens de training af. Drie maanden later vraagt de fbi Mashal naar een hotel te komen. Als hij informant wordt, zullen ze hem van de lijst halen. Hij wil eerst een advocaat spreken en benadert de American Civil Liberties Union (aclu). Die is niet verbaasd over zijn verhaal; ze heeft namelijk contact met dertien anderen die precies hetzelfde is over-komen. De aclu voegt hem toe aan een gezamenlijke rechtszaak. Na vier jaar wordt Mashal van de lijst gehaald. Vier jaar heeft hij dankzij zijn vliegverbod bruiloften, begrafenissen en zakelijke opdrachten gemist.

**OP 21 MAART STEMMEN WE** over de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten

(**Wiv**), maar in de aanloop naar dat referendum lijken we de verkeerde discussie te voeren. Het debat gaat vooral over het 'sleepnet' dat het opscheppen van gegevens via internetkabels mogelijk maakt; over de vraag of de aivd straks onze mailtjes leest en of het toezicht daarop wel op orde is. Door hierop in te zoomen, wordt een belangrijkere vraag niet gesteld; namelijk of deze vorm van massale gegevensverzameling wel werkt.

Het korte antwoord daarop is volgens veel experts namelijk: nee. Het werkt contraproductief om steeds meer hooi te gooien boven op die ene speld die je zoekt. De genoemde no fly list

bijvoorbeeld is onderdeel van een nog veel langere *terrorist watch list.* Amerikaanse overheidsdiensten selecteren uit grote gecombineerde datasets mensen die extra gescreend worden. Dat levert veel verkeerde aanwijzingen op - zoals mensen met dezelfde naam als een verdachte. Ook twee Rotterdammers kwamen er afgelopen zomer mee in aanraking: ze mochten na zes uur ondervraging Amerika ondanks hun visum niet in. De reden? Een van hen, docent Engels en komiek Ismail Aghzanay, was naar Mekka geweest. 'We werden behandeld als criminelen, als terroristen', zei hij.

Dit soort lijsten met potentiële dreigingen komt tot stand door computeranalyses van bergen gegevens die diensten ook met elkaar uitwisselen. De kans op fouten bij die automatische analyse is groot en mensen ondervinden er schade van. Dat zou acceptabel kunnen zijn als *big data-* analyses aanslagen kunnen voorkomen, maar het bewijs daarvoor ontbreekt.

*'Data mining is simply the wrong tool for the job',* schreef Bruce Schneier in 2015. Deze internationaal vermaarde veiligheids- en big data-expert is verbonden aan Harvard en ibm en adviseerde de Amerikaanse overheid. Datastapelen werkt volgens hem wel als je creditcard- of belastingfraude op wil sporen, maar niet als je tussen miljoenen mensen die ene terrorist probeert te vinden. De miljarden die aan massasurveillance worden uitgegeven noemt hij verspild geld: het levert niet de veiligheid op die wordt beloofd.

Anderen wijzen op de grote kans op fouten bij het analyseren van big data. De kans op verkeerde verdachten en op blindheid voor risico's die we nog niet kennen is groot. Het kan leiden tot discriminatie en schade voor onschuldige burgers; met rechtszaken tot aan het Europees Hof voor de Rechten van de Mens toe. Platform Investico vergeleek voor *De Groene Amsterdammer* en *Trouw* hoe veiligheidsdiensten zowel in Europa als in Amerika op zoek gaan naar dreigingen in big data. Werkt de methode en welke onbedoelde, nadelige gevolgen heeft ze? Hoe doen we het in Nederland en wie houdt er toezicht op?

**IN DE NIEUWE WIV** staat voor het eerst de geautomatiseerde verwerking van data beschreven. Big data hebben volgens de diensten een grote potentie 'omdat tegenwoordig steeds meer data automatisch worden geproduceerd en het onvermijdelijke bijproduct zijn van dagelijkse handelingen van bijna alle burgers, zoals het gebruik van internet, social media, mobiele telefoons en daaraan verbonden applicaties'. De toepassing van big data levert volgens de diensten grote tijdwinst op en geeft nauwkeuriger resultaten, waardoor aanslagen sneller kunnen worden gereconstrueerd en terroristische voornemens sneller in kaart gebracht kunnen worden.

Het interessante is dat de toelichting op de wet de valkuilen van big data-analyse wel benoemt - zoals correlaties verwarren met causaliteit, stigmatisering, discriminatie en het zogenoemde *'chilling effect'* (mensen gaan zich anders gedragen als ze zich voortdurend bekeken voelen) - maar extra toezicht is volgens de diensten niet nodig. Een team van wetenschappers en onderzoekers dat de privacyrisico's van de nieuwe wet inschatte, adviseerde dat de minister vooraf toestemming moet geven voor big data-analyse. De reactie van de diensten? 'Dat achten wij een te vergaande eis, omdat gegevens-verwerking de essentie betreft van het werk van de inlichtingen- en veiligheidsdiensten.'

Hoe effectief de big data-analyse is en hoe het risico van fouten wordt geminimaliseerd wil de aivd niet laten weten. Dat zou te veel inzicht geven in haar werkwijze. In een reactie op onze vragen stelt de dienst dat 'we pas vanaf het moment dat de wet ingaat echt aan de slag gaan met de bevoegdheden die erin staan en precies ervaren hoe een en ander werkt. Het is dus te vroeg om daar al uitspraken over te doen.'

Dat is gek, want uit diverse toezichtsrapporten, vacatures van de aivd, en de aanschaf van 'Argo II' in 2013, een softwaresysteem om grote hoeveelheden gegevens te kunnen verwerken, valt op te maken dat de diensten al jaren gebruik maken van geautomatiseerde data-analyses. Ook zonder sleepnet hebben ze nu al veel data tot hun beschikking die je alleen nog maar met behulp van big data-software kunt bekijken. Gerichte taps op de internetkabel zijn al toegestaan, net als het opvragen van informatie bij bedrijven - direct of via informanten. Veel informatie op het internet is bovendien openbaar. De inlichtingendiensten maken bijvoorbeeld gebruik van sociale-media-analyses en kopiëren complete webfora. Ze mogen ook hacken en niet-openbare informatie opkopen. Zo kochten de diensten twee datasets met elk de persoonsgegevens van meer dan

honderd miljoen mensen op het dark web, bleek afgelopen maand uit een toezichtsrapport van de ctivd.

Ook hebben overheidsdiensten toegang tot veel persoonsgegevens. Binnen de zogeheten Contra Terrorisme Infobox wordt bijvoorbeeld data gedeeld van onder andere de aivd, mivd, de politie, marechaussee, ind, de Fiod, het Openbaar Ministerie, de *financial intelligence unit,* de inspectie Sociale Zaken en Werkgelegenheid en de Nationaal Coördinator Terrorismebestrijding en Veiligheid. Deze bijzondere opsporingsdiensten hebben niet alleen veel persoons-gegevens, maar mogen vanaf komende zomer ook gericht afluisteren en undercoveracties uitvoeren. Al deze data kunnen op een hoop worden gegooid om er nieuwe analyses op los te laten, profielen te maken, en nieuwe dreigingen op te sporen.

Dat inlichtingendiensten honger naar data hebben, komt door de aard van hun werk, legt filosoof en jurist Marc Schuilenburg uit. Hij doet aan de Vrije Universiteit onderzoek naar veiligheid. 'De inlichtingendiensten zijn op zoek naar dingen die ze nog niet weten, of zoals voormalig defensieminister Donald Rumsfeld het in 2002 zo mooi verwoordde, het gaat om *the unknown unknowns.'* De inlichtingendiensten gaan op zoek naar dingen waarvan ze niet weten dat ze ze niet weten. Ze zijn op zoek naar iedere dreiging en dat kan van alles zijn. Volgens Schuilenburg is het de meest vage en ook de meest brede categorie van voorspellen: 'Je wilt bijvoorbeeld ver voor 9/11 al hebben voorspeld dat terroristen met gekaapte passagiersvliegtuigen een aanslag kunnen plegen. Maar voor 9/11 had nog niemand over die mogelijkheid nagedacht.'

Om onbekende dreigingen in kaart te brengen willen de diensten dus steeds meer gegevens verzamelen. Maar volgens Schuilenburg ligt het oneigenlijk gebruik van data op de loer: 'Als je bulkinformatie verzamelt ga je waarde hechten aan onbelangrijke dingen of aan correlaties die er niet zijn. Je gaat op zoek naar alles wat potentieel bedreigend kan zijn en daarmee steeds meer betekenis geven aan de samenhang van talloze niet-strafbare feiten. Wat je dan uiteindelijk krijgt is een gedachtepolitie.'

**MUHAMMED RABBANI IS** niet verbaasd als hij op 20 november 2016 bij de douane op -Heathrow Airport wordt aangehouden. Hij is het gewend: 'Na de twintigste aanhouding ben ik opgehouden met tellen', vertelt de directeur van de Engelse moslimbelangenorganisatie Cage. De douane beveelt hem zijn laptop en telefoon te ontgrendelen, maar Rabbani weigert. Op zijn laptop staat een hoop informatie over zijn werk en hij wil niet dat die in verkeerde handen belandt. Rabbani wordt veroordeeld en krijgt een geldboete. 'Dat is mijn terroristische daad, dat ik mijn wachtwoorden niet wilde vrijgeven', zegt hij.

Volgens EU-commissaris Mario Oetheimer worden er in heel Europa steeds meer data verzameld. De meeste landen hebben de bevoegdheden voor dataverzameling recent verruimd. In bijna alle lidstaten mogen de veiligheids- en inlichtingendiensten data van de kabel en ether verzamelen en voor langere tijd opslaan.

Telecombedrijven zijn verplicht metadata voor een langere periode op te slaan, voor het geval dat later toch nog nuttig blijkt. Landen verzamelen niet alleen zelf data, ze wisselen die ook uit met bondgenoten. Na recente aanslagen is de dataruilhandel binnen Europa verder toegenomen. Daarnaast zijn luchtvaartmaatschappijen sinds 2016 verplicht om alle passagiersdata met de Europese lidstaten te delen.

In Engeland begint de dataverzamelwoede direct aan de grens. Sinds Schedule 7 van de Britse Terrorism Act 2000 van kracht ging is het de grenspolitie toegestaan mensen zoals Muhammed Rabbani aan te houden en te fouilleren. Het leidt tot een grootschalige inbreuk in de digitale levens van onschuldige mensen. Toezichthouder David Anderson waarschuwde in 2014 dat de Engelse wet terrorisme zo breed definieert dat ook journalisten, bloggers en kennissen van vermoedelijke terroristen daar onder kunnen vallen.

Uit onderzoek van online nieuwsplatform The Intercept bleek dat de politie de verzamelde data maandelijks deelt met de Engelse inlichtingendienst gchq. Tussen 2009 en 2016 werden in Engeland gemiddeld vijftigduizend mensen per jaar aan de grens aangehouden, zonder opgaaf van redenen. Ze mogen zich niet beroepen op hun zwijgrecht en zijn bovendien verplicht elektronische apparaten aan de politie te overhandigen.

Volgens politici en veiligheidsdiensten zijn die data nodig om terrorisme te bestrijden. Zo zei de Britse premier Theresa May in 2017: 'We moeten er alles aan doen om het risico van extremisme online te verminderen.' De inlichtingendiensten stellen dat ze zonder 'bulkinterceptie' en data-analyses hun taken niet goed kunnen uitvoeren.

Het Hooggerechtshof sprak zich eind januari negatief uit over de verzameldrift van de Britse diensten. De overheid overtreedt de wet door het verzamelen van 's lands internetactiviteiten en belgegevens, en door overheidsdiensten toegang te geven tot persoonlijke gegevens van mensen die niet verdacht worden van misdaden. Het Hof oordeelde dat belangrijke delen van de 'Snoopers' Charter', zoals de Britse **sleepwet** heet, onrechtmatig zijn.

Ook in Frankrijk viert de verzamelwoede hoogtij. Als de Franse regering na de aanslag in Parijs in 2015 de noodtoestand uitroept, mag de politie zonder tussenkomst van een rechter huizen doorzoeken. In twee jaar tijd doorzoeken ze 4457 huizen. Aanvankelijk is het ook toegestaan om data uit apparaten en computers te halen die de politie in de huizen aantreft. 'Voor ons is het beste gedeelte [van de huiszoekingen] de data', getuigde Charles-Antoine Thomas, een Parijse officier, voor de Assemblée Nationale. 'Mensen slapen niet met hun kalasjnikov.'

Na het uitroepen van de noodtoestand gebruikte de Franse overheid de extra bevoegdheden om klimaatactivisten preventief huisarrest te geven en demonstraties te verbieden. Privacy International diende een half jaar geleden bij het Europees Hof voor de Rechten van de Mens een zaak in tegen de Franse overheid, omdat volgens hen automatische data-analyses en hacken in strijd zijn met de mensenrechten. Diverse Nederlandse organisaties hebben een gezamenlijke rechtszaak aangekondigd tegen de nieuwe inlichtingenwet. Ook de Raad van State vroeg zich in een reactie op de nieuwe inlichtingenwet af of de grootschalige gegevensverzameling wel voldoet aan de proportionaliteitseis van het Europees Verdrag voor de Rechten van de Mens. Het Hof in Straatsburg oordeelde in eerdere zaken dat massasurveillance zeer ingrijpend is omdat primair gegevens van onschuldige burgers worden verzameld.

**ALS JE AL DIE GEGEVENS** hebt, wat doe je er dan mee? Het makkelijkste is ze te doorzoeken op dreigingen die al bekend zijn: een persoon van wie je weet dat hij of zij kwade plannen heeft. Maar dat is doorgaans niet wat inlichtingendiensten doen, zij moeten juist op zoek naar de dreigingen die nog *niet* bekend zijn. Kon je als aivd'er vroeger nog handmatig je dossiers opbouwen en puzzelstukjes samenvoegen, dat is met de hoeveelheid gegevens van vandaag de dag niet meer te doen. Je hebt dus hulp nodig van data-analisten en van slimme software.

In Amerika, Frankrijk en vele andere landen wordt hiervoor aangeklopt bij het bedrijf Palantir. Deze 'Rolls Royce van de big data' is in handen van tech-miljardair Peter Thiel en kwam mede tot stand dankzij een investering van de cia. Het is na de leaks van Edward Snowden wel omschreven als het systeem dat de Amerikaanse dienst nsa helpt de hele wereld te bespioneren. Met het programma Palantir Gotham kunnen overheden snelle analyses maken in één gecentraliseerde database, waar je een boel gevoelige informatie met één klik kunt doorzoeken, én gemakkelijk informatie tussen landen kunt delen.

Andere overheden maken gebruik van HackingTeam, een commercieel Italiaans bedrijf dat zijn diensten aan ieder land verkoopt dat wil betalen. Met de software van HackingTeam kun je apparaten hacken, maar bijvoorbeeld ook digitaal verkeer ontsleutelen. Dat wordt niet alleen gebruikt om terroristen te slim af te zijn, maar ook om journalisten, dissidenten en mensenrechtenactivisten mee op de huid te zitten.

Dat het onderbrengen van grote hoeveelheden gegevens bij commerciële bedrijven ook risico's met zich meebrengt, bleek in 2015 toen HackingTeam zelf gehackt werd door een ethische hacker die vierhonderd gigabytes aan informatie buit maakte.

Experts als Bruce Schneier wijzen erop dat de technische kennis om te hacken, virussen te verspreiden of op grote schaal online te surveilleren aanvankelijk door overheden wordt gefinancierd, maar daarna vaak in verkeerde handen valt. Een bekend voorbeeld is het door Amerikanen ontworpen virus Stuxnet dat een Iraanse nucleaire fabriek plat moest leggen, maar in Iraanse handen terechtkwam. Zo ontstaat een nieuwe digitale wapenrace, en maakt veel van de inbraak- en analysesoftware die overheden gebruiken de wereld uiteindelijk onveiliger. Omdat

diensten makkelijk bij gegevens willen kunnen, hebben ze bovendien geen belang bij het veiliger maken van gegevensopslag of verwerkingssystemen.

**IN NEDERLAND WETEN WE** niet precies hoe de diensten hun gegevens analyseren en met welke bedrijven ze samenwerken, daarover wil de aivd geen uitspraken doen. Uit een recente vacature blijkt dat de aivd big data-engineers aanneemt die software kunnen ontwikkelen om grote hoeveelheden data te verwerken. We weten ook dat in 2013 software is aangekocht met de codenaam 'Argo II' om van 2014 tot 2018 te kunnen gebruiken. Argo II is vooral bedoeld om 'de wereld van het internetprotocol' te bestrijken, bleek uit een omschrijving van het ministerie van Defensie. Wat weer tot Kamervragen leidde omdat de diensten hiermee op het 'sleepnet' vooruit leken te lopen. Journalisten herleidden de software destijds tot het Israëlische bedrijf Nice Systems, maar de overheid wilde dat niet bevestigen. Nice Systems zelf zegt bij navraag dat de betreffende divisie in 2015 is door-verkocht aan de Amerikaanse privaty-equityfirma Battery Ventures.

Wie wel toelichting wil geven over zijn software is de Nederlandse Peter de Kock van Pandora Intelligence. Dat bedrijf won een innovatiewedstrijd van het ministerie van Defensie en kreeg twee ton om een geautomatiseerd scenariomodel verder te ontwikkelen. De Kock werkte eerder bij de politie en als filmmaker en benadert terroristische aanslagen als filmscenario's. Hij voegde de kleinste details van alle terroristische aanslagen die hij kon vinden samen met romans, sciencefiction en films over aanslagen. Dat leidde tot een complex systeem waar algoritmes overeenkomsten of trends in kunnen ontdekken. Stel dat er ergens een aanslag gepleegd wordt en er zijn nog maar een paar details bekend, dan kan De Kocks model daar het meest waarschijnlijke scenario bij leveren.

Volgens Peter de Kock kunnen we het ons niet veroorloven geen gebruik te maken van algoritmes. 'Een systeem kan misschien wel beter uitleggen hoe dat tot een bepaalde beslissing is gekomen dan een mens.' Het lastige is: ingewikkelde algoritmes zoals die van De Kock zijn zelflerend. Ze ontwikkelen zich steeds verder waardoor zelfs specialisten ze steeds minder snappen. 'Daarom moet je ze transparant maken en altijd blijven controleren', zegt De Kock.

Experts zetten hun vraagtekens bij de betrouwbaarheid van algoritmes om terroristen op te sporen. Waar bedrijven als Amazon en Google dagelijks zoveel transacties en zoekopdrachten uitvoeren dat ze constant kunnen checken of hun algoritmes de juiste suggesties doen, komt terrorisme relatief weinig voor. De Deense onderzoeker Timme Munk beaamt dit: 'Het is lastig om gebeurtenissen te voorspellen die nauwelijks voorkomen. Daar komt bij dat we nauwelijks weten wanneer en hoe iemand met extremistische denkbeelden uiteindelijk terrorist wordt.' In een wetenschappelijke studie rekende hij voor dat voor iedere potentiële terrorist wel honderdduizend 'verkeerde' verdachten moeten worden gecheckt.

Neem Skynet, een nsa-programma dat automatisch terroristen in kaart moest brengen. Het had volgens gelekte Powerpointslides een foutpercentage van slechts 0,18. Toch betekent dat op een database van 55 miljoen personen dat het systeem 99.000 personen onterecht als terrorist aanmerkt. Al die mensen zoals Mashal en Rabbani moeten nader worden gecheckt. Dat maakt dit soort methodes omslachtig, tijdrovend en duur. Hoe meer data je verwerkt, hoe groter de kans op fout-positieven bovendien wordt.

'Bij ieder algoritme maak je een keuze tussen meer fout-positieven (onschuldigen die als verdacht worden aangezien) of meer fout-negatieven (terroristen die voor onschuldig worden aangezien)', zegt Munk. 'De politieke druk is momenteel zo groot dat we meer fout-positieven accepteren. Zo worden onschuldige mensen schuldig bevonden, totdat ze kunnen bewijzen dat ze dat niet zijn.'

**EEN MOEDER EN HAAR BABY** worden uit de rij geplukt op het vliegveld van Detroit. De moeder moet haar tas omkeren en alle luiers worden één voor één gecheckt. Haar zeven maanden oude zoontje krijgt een rigoureuze inspectie en wordt gefouilleerd. De reden? Het ventje staat op de terrorist watch list. Het verhaal van 'Baby Doe' komt terug in een gezamenlijke rechtszaak die in 2016 werd aangespannen tegen onder andere het Terrorist Screening Center. Onder de aanklagers bevinden zich opvallend veel mensen uit Dearborn, een rustig Amerikaans stadje in de staat Michigan. Alles bij elkaar wonen hier nog geen honderdduizend mensen, van wie de meesten in de auto-industrie werken. Dearborn dankt zijn faam namelijk aan Henry Ford die er opgroeide en er het hoofdkwartier van Ford stichtte, dat er nog altijd staat.

Maar twee jaar geleden kwam Dearborn om een heel andere reden in het nieuws: het is na New York de stad met de meeste mensen op de Amerikaanse terrorist watch list. De reden? Dearborn heeft voorzover we weten nog nooit een terrorist geproduceerd, maar heeft wel een grote moslimpopulatie. Een plek op deze lijst blijft niet zonder gevolgen, want hij wordt ook met andere instanties gedeeld. Veel genoemde problemen: gedoe bij de aanvraag van een rijbewijs, niet door de douane komen, -bankrekeningen die bevroren worden en geweigerde leningen.

**OMDAT ALGORITMES GEVOED** worden met historische gegevens hebben ze de neiging vooringenomenheid of bias te versterken. Zo deed de journalistieke organisatie Propublica in 2016 onderzoek naar een criminaliteitsvoorspeller in de VS die liet zien dat deze vorm van geautomatiseerde data-analyse het vooroordeel tegen zwarte jongemannen versterkt, waardoor zij eerder worden opgepakt en zwaardere straffen krijgen.

Wat gebeurt er als je hetzelfde doet met gegevens van terroristen? tno-onderzoeker Selmar Smit deed veel onderzoek naar big data en algoritmes, onder andere voor de politie en andere veiligheidsorganisaties. 'Een woninginbraak kun je goed voorspellen omdat het mensen zijn die zelf aangifte doen, ongeacht het eventuele profiel van de inbreker. Maar bij staandehoudingen van de politie is het al weer anders. Dat werkt niet als je die in een systeem invoert omdat je zo de bias van agenten versterkt. Stel dat je bij terroristische aanslagen alleen de gegevens invoert van de daders die je pakt. Dat zijn misschien wel de domme terroristen. Dan is zo'n systeem blind voor andere daders. Dus zelfs bij zoiets simpels kun je de mist in gaan.'

Hij geeft nog een voorbeeld: IS en al-Qaeda zijn de bekendste terroristische groepen, er is veel over ze bekend en ze posten zelf veel filmpjes op YouTube. 'Maar als je alleen bekende gegevens invoert, krijg je er ook vooral dat soort voorspellingen uit. Het gevaar van big data-analyse bij terrorisme is dus dat je alleen nog maar op zoek gaat naar bekende jihadisten en andere vormen van radicalisme over het hoofd ziet. Of dat je alleen nog maar oog hebt voor de "domme" terroristen die zich laten pakken, omdat zij oververtegenwoordigd zijn in je historische gegevens. Mensen zijn eerder geneigd om buiten de box te denken. Computers doen gewoon precies wat we van ze vragen.' Gelukkig is er een instantie die, onder de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten, onze diensten moet controleren op de mogelijke fouten en valkuilen bij big data-analyse. Die verantwoordelijkheid ligt bij toezichthouder ctivd, die het werk van de diensten achteraf toetst.

In de nieuwe wet wordt 'geautomatiseerde data-analyse' omschreven als een 'algemene bevoegdheid', niets bijzonders dus. Alleen beslissingen mogen niet volledig geautomatiseerd genomen worden: er moet altijd een mens aan te pas komen. Voor geautomatiseerde dataanalyse is dus géén toestemming nodig van de minister of van de nieuwe Toetsingscommissie Inzet Bevoegdheden (tib). Alleen als de data zijn verzameld met het veelbesproken 'sleepnet' moet dat wel: zowel de minister als de tib moet eerst de tap goedkeuren, en vervolgens de geautomatiseerde data-analyse van die tap.

De ctivd kijkt achteraf naar rechtmatigheid - klopt het volgens de wet? - maar gaat ook de betrouwbaarheid en kwaliteit van gegevensverwerking toetsen. Hoe? Dat weet ze nog niet, want de diensten moeten dit eerst zelf uit-- vogelen, het staat namelijk niet in de wet omschreven.

'De hele **Wiv** hangt vol met toezicht, maar we controleren niet de tools op grond waarvan de veiligheidsdiensten beslissingen nemen. Dat blijft een black box', waarschuwt filosoof en jurist Marc Schuilenburg. 'De toezichtsinstantie doet straks een rechtmatigheidscontrole; mag het volgens de wet? Maar wat ze eigenlijk zouden moeten doen is een doelmatigheidscontrole. Werkt het wel? En hoe zorg je er bijvoorbeeld voor dat je zo veel mogelijk missers uitsluit?'

**OUD-MINISTER** Ernst Hirsch Ballin benadrukte het probleem van automatisering toen hij in 2016 de fraaie zin *'alleen computer says yes or no is onwenselijk'* uitsprak. Hij presenteerde het wrr-rapport *Big data in een vrije en veilige samenleving,* waarin bijna alle bezwaren van big data-analyse door overheid en inlichtingen- en veiligheidsdiensten staan samengevat. Burgers krijgen het gevoel dat hun vrijheid wordt ingeperkt en persoonlijke levenssfeer aan-getast. Dit kan leiden tot een chilling effect op de grondrechten. Deze effecten worden versterkt omdat de methoden en technieken van big dataanalyse nauwelijks zichtbaar zijn. De profilering van groepen burgers kan tot discriminatie en oneerlijke behandeling leiden en tot verkeerde conclusies. De wrr wijst ook op het gevaar

van *'function creep':* het is verleidelijk om gegevens te gebruiken voor een ander doel dan waarvoor ze verzameld zijn.

In een voorstudie van dit rapport dook onderzoeker Sascha van Schendel van de Universiteit Tilburg in de wereld van inlichtingendiensten en big data. Daarin haalt ze een aantal missers aan. De militaire inlichtingendienst mivd gebruikte in 2011 bijvoorbeeld te breed geformuleerde profielen om nieuwe communicatie via de ether te verzamelen. Ze citeerde ook de conclusie van de toezichthouder ctivd dat 'bijzondere bevoegdheden (...) een technologisch steeds geavanceerder inbreuk maken op de privacy van burgers'. Bij inlichtingenoperaties op sociale media werd bijvoorbeeld niet altijd goed met privacybescherming omgegaan. Daarnaast constateerde de toezichthouder dat het heimelijk binnenhalen van data van een aantal grotere algemene webfora disproportioneel en dus onrechtmatig was.

Sascha van Schendel maakt zich zorgen over de nieuwe inlichtingenwet. 'Zoals ik de wet nu lees, zullen de diensten alleen maar meer profielen gaan maken. Maar hier zijn grote risico's aan verbonden. Kan dat profiel wel honderd procent kloppen? Die zorg is in de nieuwe wet veel te makkelijk afgedaan met het antwoord: "We zetten wel een persoon naast de computer." Maar het is belangrijk dat je als mens snapt hoe alle stappen zijn gemaakt en hoe zo'n profiel ontstaat. We zien in de Verenigde Staten dat het wel degelijk nadelige gevolgen kan hebben voor mensen als ze verkeerd geprofileerd worden.' De kans dat onschuldige burgers geprofileerd worden, neemt volgens Van Schendel toe als er straks onder de nieuwe wet meer data binnengehaald worden door hacks of bulkinterceptie via de internetkabel. De discussie over de effectiviteit van deze methoden is volgens haar nooit gevoerd in Nederland: 'Misschien weten de diensten zelf ook niet hoe effectief het is.'

Als er één iemand is die wél geprobeerd heeft die discussie over effectiviteit te voeren, is het voormalig pvda-politica Astrid Oosenbrug. Zij stemde als enige van haar partij tegen de **Wiv** in de Tweede Kamer. 'De noodzaak van meer data verzamelen is me in al die debatten niet duidelijk geworden', zegt ze. Zowel de verantwoordelijke ministers als medewerkers van de veiligheidsdiensten konden Oosenbrug (die een ict-achtergrond heeft en tegenwoordig een cyberwerkplaats runt) hiervan niet overtuigen. 'Je gaat zoeken naar een speld in een nog grotere hooiberg. Ik wilde echt wel overtuigd worden, maar niemand heeft me uit kunnen leggen waarom dit nodig is.'

Volgens haar zijn er in de Tweede Kamer niet de juiste vragen gesteld bij de wet. Dat komt volgens haar door een gebrek aan technische kennis bij politici. 'Het is onvoorstelbaar dat Kamerleden zeggen dat je helemaal geen ictkennis hoeft te hebben als je ict-woordvoerder bent. Stel je voor dat iemand op zorg zegt: "Een ziekenhuis, medicijnen, nog nooit van gehoord." Dat kan toch niet? Als je in de Kamer niet de juiste kennis in huis hebt, dan kun je ook niet de juiste vragen stellen.'

Politici zijn volgens haar bang dat onder hun verantwoordelijkheid de veiligheidsdiensten iets over het hoofd zien. Het resultaat: ze staan toe dat de diensten steeds meer gegevens binnenhalen. Maar, zegt Oosenbrug: 'Je kunt niet met nog meer data de veiligheid vergroten. Wat je biedt, is een schijnveiligheid en daar ben ik gewoon niet van. Mensen krijgen bovendien het idee dat ze continu bekeken worden en passen hun gedrag aan. Uiteindelijk is iedereen dan verdacht, en dan leven we in een onvrije wereld.'

De wrr waarschuwde voor precies deze effecten, en pleitte daarom voor meer waarborgen bij big data-analyse om het vertrouwen in de samenleving te behouden. Maar hoe doe je dat? Daarvoor hoeven we misschien alleen maar twee landen verder te kijken. We spraken eerder al over de verzamelwoede van Frankrijk, maar in dat land is in 2015 óók afgesproken dat onder de nieuwe inlichtingenwet big data-analyse alleen voor anti-terrorisme-activiteiten is toegestaan, en alleen met toestemming van de premier. Ook moet een commissie vooraf een (niet-bindend) advies geven. Deze toestemming geldt slechts voor twee maanden en mag alleen verlengd worden als het algoritme niet te veel fout-positieven oplevert.

Hoogleraar ethiek en technologie Jeroen van den Hoven van de TU Delft benadrukt dat je gegevensanalyse zo kunt inrichten dat het zowel de privacy, rechtvaardigheid en -waardigheid als veiligheid ten goede komt. 'We moeten af van dat denken dat veiligheid altijd ten koste van privacy moet gaan. Je kunt systemen zo -inrichten dat ze en/en/en waarborgen. Daar liggen de mogelijkheden voor echt verantwoorde innovatie.'

Van den Hoven vindt dat de overheid juist moeite moet doen om over de data-analyse - de 'black box' - verantwoording te kunnen afleggen. 'Mensen vinden het prima als hun gegevens echt alleen voor bevordering van de veiligheid verzameld worden, en als er voldoende waarborgen zijn om fouten en misbruik van algoritmes te voorkomen. Dat zou al een enorme angel uit deze wet halen.'

**Sleepwet 1 oktober 2017 (1 uur en 6 minuten)**
Lubach: We moeten het hebben over een nieuwe wet, de wiv. Dan denken jullie weet ik veel? Bijna goed. Maar het staat voor wet op de inlichtingen en veiligheidsdiensten. Dat is de nieuwe wet die bepaalt wat de geheime diensten allemaal mogen. Nou, wat betekent dat voor ons?

Fragment: Geheime diensten zoals de aivd mogen vanaf 1 jan 2018 iedereen afluisteren

Lubach: Antoinette niet zeggen dat het de aivd is dan is het toch geen geheime dienst meer

Fragment: Bevoegdheden van de geheime diensten worden flink uitgebreid, zo mag er een zogenaamd sleepnet worden ingezet om massaal online communicatie af te luisteren, ook van niet verdachte personen. Een hele wijk kan worden afgeluisterd wanneer er 1 verdacht persoon in woont. Telefoons, computers en zelfs smart-tv's mogen gehacked worden.

Lubach: Ja, en dat is ernstig want als ze mn smarttv hacken zien ze dat ik de hele dag tros-radar zit te kijken. Dat was echt belachelijk laatst, met de koelkast, ik weet het ook niet meer. De nieuwe wet was nodig omdat de oude wif achterhaalt is. Die is al meer dan 15 jaar oud. En toen, toen zag de digitale wereld er heel anders uit. Toen waren enzo knol en dee nog niet uit elkaar. Ook nog niet bij elkaar trouwens, maar dat maakt niet uit… Of geboren. Een hele andere tijd dus.

Fragment: De oude wet is van 2001, even terug naar 2001, geen facebook, geen whatsapp, we communiceerden hoofdzakelijk nog via de telefoon of smsjes.

Lubach: Ja, die tijd. Geen facebook, geen whatsapp. Dat kunnen jongeren van nu zich helemaal niet meer voorstellen. Als ik een dickpick de klas rond wilde sturen moest ik hem 25 keer printen en iedereen op de post doen. Fucking veel werk. De oude wif ging vooral over de draadloze communicatie, via de satelliet bijvoorbeeld. Maar tegenwoordig gaat bijna alles via de glasvezelkabel. En de nieuwe wet bepaalt wanneer die kabel mag worden afgetapt. De geheime diensten willen dat, om ons goed te kunnen beschermen, bijvoorbeeld tegen buitenlandse hackaanvallen. Zoals deze:

Fragment:
Momenteel halen digitale speurders de laatste resten Iraanse malware van de servers van een nederlandse vestiging van een internationaal telecombedrijf. De Iraniers hebben maandenlang in de systemen gezeten en waardevolle informatie kunnen wegsluizen.

Lubach: Ja, iran had dus in nederland een soort virus geplaatst bij een telecombedrijf. Met de nieuwe wet kunnen de geheime diensten bij de hoofdkabels van het internet checken of dat virus ook bij andere bedrijven is geinstalleerd. en dat is best wel nuttig. (...) En wat ook wel handig is, als nederlanders in syrie vechten en ze praten met hun vrienden in nederland via een bepaalde app, dan kan de aivd straks alle commmunicatie via die app afstappen tussen syrie en nederland, en dan kijken wie met wie in contact staat. klinkt super handig. Aan de andere kant, als er ergens een aanslag is geweest, dan lees je achteraf altijd weer dit: De dader was al in beeld. (...) En dat hoor je dus altijd ná een aanslag. Dus de diensten

hebben blijkbaal al meer gegevens dan ze kunnen analiseren. De britse geheime dienst heeft zelfs last van te veel data. Meer data betekent dus niet altijd meer veiligheid. En het wordt nog erger, want de nieuwe wif is net als hiv, niet iedereen is er blij mee. En dat heeft hier mee te maken:

Fragment: Wat wel zo is, is dat de verzameling van informatie redelijk grof is en dat daar niet alleen maar terroristen of mensen met verkeerde bedoelingen in zitten.
- Dus daar zitten ook mensen bij die helemaal niks gedaan hebben?
De informatie van die mensen zit daar zeker bij.

Lubach: Ja, ze gaan dus niet allen verdachten aftappen maar ook onschuldige mensen zoals, u. En dat onderdeel van de wif wordt ook wel het sleepnet genoemd. Als je straks is een bepaalde wijk woont waar toevallig ook wat syriegangers vandaan komen dan mag de aivd een digitaal net uitgooien en bestaat de kans dat ook jouw internetverkeer wordt opgevist. (...) De term sleepnet wordt vooral gebruit door tegenstanders van de wif. Maar het woord sleepnet staat natuurlijk niet zo in de wet zelf. Daar stond het eerst zo: Ongerichte interceptie. Maar ongericht  klinkt natuurlijk een beetje lomp. Dus dat hebben ze heel slim veranderd naar ‘doelgerichte interceptie’. Klinkt al beter, vooral omdat het precies het tegenovergestelde betekent. Maar dat vonden ze ook een beetje te ver gaan, dus als je nu de wet er bij pakt staat er ‘onderzoeksgericht onderzoek’. (...) Er is nog iets geks aan de hand met die wif. Want al die data van die onschuldige mensen wordt natuurlijk ergens opgeslagen. Maar voor hoe lang? In duitsland gebeurt dat meestal 90 dagen, en in engeland een half jaar, maar hoe lang mag het van de nieuwe wif? Dat is 3 fucking jaar, meer dan 1000 dagen. En dan heb ik het dus niet over de gegevens van criminelen, maar echt over (...) de gesprekken tussen jantje en klaasje. Die mogen dus heel lang worden bewaard. Het enige voordeel wat ik kan verzinnen is dat je straks drie jaar na dato nog naar de aivd kan gaan om te vragen waarom het uit is gegaan met je vriendin. (...) Maar goed, er komen dus digitale sleepnetten en de aivd hoeft dus onschuldige vissen pas na 3 jaar terug te gooien. Minster Plasterk is de baas van de aivd. (...) Wat zegt hij over het sleepnet?

Fragment: Het mag alleen maar als de minister van te voren toestemming geeft voor een bepaalde doelgerichte actie.

Lubach: Oke, dus de minister moet toestemming geven, en hij bepaalt wat er precies mag worden onderschept. Maar wie controlleert dan de minister?

Fragment: De wet geldt, dus ook in een situatie dat de druk groot is, moeten de diensten zich echt aan de wet houden we hebben ook nog eens een toezichthouder….

Lubach: Oke, de wet dus, en er is ook een toezichthouder. Om te kijken of de minister zich aan die wet houdt. En dan is er ook nog een speciale commissie die achteraf kijkt of het allemaal wel volgens de wet is gegaan. Klinkt opzich goed, maar, wat zegt die commissie er van? “Om effectief toezicht uit te kunnen oefenen, moet er echter sprake zijn van een duidelijk en afgebakend kader in de wet. Dat is nu niet in ieder geval.” Dus de commissie zelf vindt die wet te vaag. Dus we krijgen straks een nieuwe wet, maar die wet is een beetje vaag, dus bepaalt de minister wat er mag samen met de toezichthouder maar omdat die wet nogal vaag is worden zij gecontroleerd door een commissie en die moet alles achteraf checken in de wet, die dus veel te vaag is. Ik maak me zorgen over die nieuwe wif. En ik ben niet alleen. Ook andere zeer gezachhebbende instanties hebben kritiek geuit. Check dit lijstje: Autoriteit persoonsgegevens, college voor de rechten van de mens, amnesty international, de raad voor rechtspraak, de raad van state, de wwr (...) Maar goed, iedereen

met een computer, is dus tegen. En ja, ik ook. En dan ben ik nog iemand die niets te verbegen heeft he, (...).
gee

Lubach: Nee, maar jij bent dan al lang weg. En als dat gebeurt dan moeten we bij alles wat we doen er rekening mee houden dat de overheid misschien wel meekijkt.

Fragment: Plasterk: “nee dat is zeker de bedoeling niet.”

Lubach: Nee, maar het gaat nogal vaak mis he, met de nederlandse overheid en ict.

Fragment: Plasterk: “nee dat is zeker de bedoeling niet.”

Lubach: En hackers worden elk jaar weer beter en slimmer en die zijn ook uit op onze gegevens.

Fragment: Plasterk: “nee dat is zeker de bedoeling niet.”

Lubach: Nee maar zo zijn hackers nu eenmaal. (...) En nu zeg je, ja nou en ik heb niks te verbergen. Oke, stel je krijgt op een dag een pakketje in de bus, met een camera een microfoon en een briefje er bij: ‘Hang deze apparaten op in je huis en zet ze aan, we gaan er principe niks mee doen. Groetjes de overheid.’ Wie zou die dingen ophangen? Niemand. Of stel je voor, vanaf nu elke keer als je je computer opstart krijg je dit popupscherm: ‘Vind je het goed dat de overheid al je chats en zoekopdrachten kan meelezen en opslaan? We gaan er in principe niets mee doen.’ Wat zou je dan klikken? Publiek: “Nee”. Maar we hebben al ‘ja’ gezegd, want dat is de wif. En die gaat in op 1 januari 2018. Is daar nog iets aan te doen? Nee. (...) Maar, er loopt sinds kort een actie om een referendum af te dwingen, en nee ook daarmee kunnen we die wet niet tegenhouden. Het is een raadgevend referendum, we kunnen er alleen mee zeggen (...) ‘jullie voorgangers hebben een fout gemaakt, een verkeerde wet, doe daar wat aan. Kijk dat item van zondag met lubach nog eens terug.’ En dan zeg je ‘nee maar ik ben tegen referenda’ Ja ik ook maar fuck dat even! Ik ben ook tegen wapens, maar als er een herdershond een baby ligt te verscheuren schiet ik hem ook voor zn kop. (...) Om dat referendum voor elkaar te krijgen zijn er 300.000 handtekeningen nodig, dat is veel, maar het kan. Als jullie nu allemaal tekenen op www.sleepwet.nl dan krijgt Ronald Plasterk vanavond nog het slechte nieuws.

Fragment: Plasterk: “nee dat is zeker de bedoeling niet.”

Lubach: Dat is zeker de bedoeling wel.

(...)

**Sleepwet 5 november (37 minuten)**
Lubach: Er komt definitief een referendum over de wiv (...). De nos noemt de wif trouwens de aftapwet, rlt spreekt over de tapwet en tegenstanders hebben het over de sleepwet, maar die wet heet dus de wiv. (...) Nou die wet (...) heeft niet alleen een lastige naam, ook het hele idee van een referendum is voor sommige mensen lastig. (...) Sybrand Buma gaat zich niets aantrekken van het referendum. En dat is opvallend, want vorig jaar toen hij nog in de oppositie zat bij het oekraine referendum was buma ook voor, maar vond hij nog dat de

uitslag wél gerespecteerd moest worden. Maar het komende referendum wil hij dus gewoon gaan negeren. Maar je kunt toch niet miljoenen mensen naar de stembus laten gaan, om dan vervolgens bij een ja wel en bij een nee niet te volgen.

Fragment: Buma: “Je kunt niet miljoenen mensen naar de stembus laten gaan, om dan vervolgens bij een ja wel en bij een nee niet te volgen.”

Lubach: (...) Waar het om gaat; als je een uitslag hebt kan je dat niet negeren. Je kan niet achteraf zeggen ‘ach het valt me wat tegen, we doen toch wat we willen.’ Dan is het uit met het vertrouwen.

Fragment: Buma: “Je kan niet achteraf zeggen ‘ach het valt me wat tegen, we doen toch wat we willen.’ Dan is het uit met het vertrouwen.”

Lubach: Ik vind het helemaal prima als je ‘buma’ een referendum bent, maar dat referendum is er nou eenmaal. Dat is de wet. Dat kan je niet zomaar negeren. (...) Maar goed, het is ook een hele omschakeling he, als je opeens vanaf de oppositie in de regering zit. Wie daar ook last van heeft is D66. Die waren eerst tegen de aftapwet en zijn nu voor. En ze waren voor het referendum en nu tegen. Terwijl ze het nota bene zelf hadden bedacht. D66 is dus heel erg voor directe democratie, behalve als het ook echt dreigt te gebeuren. Voor D66 zijn wij, het volk, in theorie heel erg leuk. We zijn een soort uitgaansavond die heel erg tegenvalt. (...) Tot grote teleurstelling van de coalitiepartijen komt dat referendum er dus wel. En even voor de duidelijkheid, tegenstanders vinden ook dat er een nieuwe moderne wet moet komen. Er zijn alleen nog een paar belangrijke onderdelen waar even goed naar gekeken moet worden. Het sleepnetgedeelte, het hacken van derden, risico’s voor journalisten bijvoorbeeld. Maar voor die nuance is bij de voorstanders van de wif, zoals Mark Rutte, geen ruimte:

Fragment: Rutte: “Sleepwet dit dat, pas op ze deugen niet die politici. Weet je wie er niet deugen Frits? Dat zijn die klootzakken die die aanslagen plegen.”

Lubach: (...) Dat aanslagplegers deugen, dat zegt helemaal niemand. Maar dit hoort bij de strategie van het kabinet. Kijk, het ene uiterste ligt bij een politiestaat met volledige controle zonder enige privacy. En het andere uiterste is totale privacy maar nul controle of veiligheid. En op dat spectrum zit die wiv nu *hier*, en wij willen het ietsje meer *deze* kant op. Maar het kabinet doet nu alsof we het allemaal willen afschaffen, die hele aivd weg en stoppen met terreurbestrijding. Maar dat is onzin natuurlijk. Dat ga je de komende weken vaker zien; de terreurschwalbe. Bij de minste kritiek meteen op de grond gaan liggen huilen over een aanslag. In de hoop op een vrij tap. De VVD gaf het startschot voor die aanstelcampagne door twee VVD-kanonnen lang te sturen bij Rick Nieman. Annemarie Jorritsma en Arthur Docters van Leeuwen. Die laatste is de oud directeur van de geheime dienst en ging maar meteen op de grond liggen voor een terreurschwalbe.

Fragment: - Dus als die tegenstanders van die nieuwe wet hun zin krijgen wordt Nederland direct onveiliger?
Docters van Leeuwen: “Ja, en daar zullen een aantal militairen door sneuvelen.”
- en er zullen ook aanslagen plaatsvinden?
Docters van Leeuwen: “Ja zeker”

Lubach: Ja, dat is dus de terreurschwalbe in full effect. (...) Dit is pure bangmakerij, nou dat is dan gelukt, mooie tereurschwalbe, prachtig. Maar toen, toen werd hij overmoedig.

Fragment: Docters van Leeuwen: “Ik las gisteren in de krant, financieel dagblad, dat een of andere ‘port’ aangaf dat er 40.000 plaatsen zijn op het darkweb waar je randsomware kan kopen.”

Lubach: (reageert op het feit dat Docters van Leeuwen niet goed uit zn woorden komt) En er was deze week nog maar 1 ding nóg onbegrijpelijker dan deze zin. Namelijk een motie die deze week werd aangenomen in de tweede kamer. Die luidt ‘We beloven de uitslag van het referendum serieus te nemen.’ En die motie werd ook gesteund door sybrand buma. Dus dat is die buma, die tegen referenda is, maar de uitslag van het oekraine referendum toch wilde respecteren, en de uitslag van het komende referendum wil negeren, maar nu dus wel serieus wil nemen, serieus negeren. (...)

**Zondag met Lubach 18 maart 2018 (1 uur 4 min)**
Over drie dagen is het referendum over de wiv, de nieuwe wet op de veiligheids en inlichtingendiensten. (...) Sommige mensen weten al waar ze op gaan stemmen, en anderen hebben nog geen idee waar het over gaat. (...) Tegenstanders van de wif hebben een paar bezwaren. Die wet maakt het mogelijk om onschuldige mensen te hacken om bij verdachten te komen. En ze kunnen allerlei gegevens delen met buitenlandse diensten, en dan is er ook nog het zogenaamde sleepnet, waarmee communicatie van onschuldige mensen kan worden onderschept. Er zijn nog veel meer bezwaren. D66-kamerlid Kees Verhoeven had er vorig jaar zelfs 21. 21 bezwaren, maar daar is niets mee gedaan. Dan zou je zeggen, Kees boos, maar nee. De partij van Kees zit intussen in de regering en is voor de wet. (...) Dit was Kees vroeger:

Fragment: Kees: “Voorzitter, geen sleepnet, laat ik daar mee beginnen. (...) Ik heb de afgelopen jaren en zeker weken gezien hoeveel mensen er vrezen voor een sleepnet. (...) Sleepnet (...) Sleepnet (...).”

Lubach: Ja, en dit is Kees nu:

Fragment: Kees: “Ik wil graag een inhoudelijk debat over deze wet, en laten we beginnen met de juiste naam voor deze wet. Het is de wet op de inlichtingen en veiligheidsdiensten, de wiv. De vraag van het referendum gaat niet over een sleepwet of een sleepnet, het gaat over die hele wet. Of je daar voor of tegen bent. Dus alle frames en andere onjuistheden in dit debat zou ik graag niet meer willen horen.

Lubach: Ik mis de oude Kees. (...) D66 zit nu dus in de regering en de wet wordt verdedigd door minister ollongren van binnenlandse zaken. Dinsdag zat zij bij nieuwsuur om uit te leggen waarom die nieuwe wet tóch nodig is.

Fragment: (...)

Lubach: Ollongren zegt dat de diensten niet mogen aftappen via de kabel. Dat klinkt inderdaad erg onhandig, maar het klopt niet. Dat mag namelijk wel. Wat nu nog niet mag is grote groepen tappen via de kabel als je nog niet weet wie je moet hebben. Het sleeptnet dus. Maar het gericht tappen van 1 verdachte via de kabel mag nu ook al. En dan denk je Ollongren vergist zich even, maar nee. Het is kabinetsbeleid. Premier Rutte kwam vrijdag namelijk met precies dezelfde misleiding. (...) Het probleem is dat het niet waar is. Dat het kabinet ervoor kiest om campagne te voeren door te liegen. Daar komen ze mee weg omdat het best wel een ingewikkelde wet is en omdat ze niet tegenover de meeste kritische experts

gaan zitten. Mark Rutte ging er zelfs nog een stapje verder in en besloot het volk toe te spreken met een hoge militair naast zich. Lekker zuid amerika Mark. (...) Maar goed, het volk mocht hem via facebook alles vragen. (...) De vraag is, waren die vragen een beetje kritisch?

Fragment: Rutte: “Nou, dan vraagt Berend van den Bosch ‘waarom zit er een evenwicht tussen privacy en veiligheid in deze wet?’. Nou en dat is een vraag die ik ook heel vaak krijg.”

Lubach: (...) Dat is toch geen vraag? Beste premier, even een kritische vraag over uw kapsel: waarom zit uw haar zo goed? Je zou je bijna gaan afvragen of die Berend van den Bosch niet een VVD-er is die de premier komt helpen met z’n nepvraag. Je zou dat bijna even gaan checken. (...) Berend van den Bosch is bestuurslid Promotie en Ledenwerving bij de jongerentak van de VVD in Amsterdam. Wat zijn dit voor tacktieken? De regering is dus bereid om alle middelen in te zetten. En dat zag je al in oktober toen ze Arthur Docters van Leeuwen naar voren schoven. (...) Hij was ooit de baas van de geheime dienst. En hij is voor de nieuwe wet, want anders gaan we allemaal dood. En dat ziet er ongeveer zo uit.

Fragment: - Dus als die tegenstanders van die nieuwe wet hun zin krijgen wordt Nederland direct onveiliger?
Docters van Leeuwen: “Ja, en daar zullen een aantal militairen door sneuvelen.”
- en er zullen ook aanslagen plaatsvinden?
Docters van Leeuwen: “Ja zeker”

Lubach: Weet je nog, dit noemde we een terreurschwalbe. (...) De zuiverste terrreurschwalbe dit seizoen werd gemaakt in de tweede kamer. Daar was een debat over de wiv tussen Gert-Jan Segers en Geert Wilders. Nou, wat zegt die enge populist?

Fragment: Segers: “Als er (...) een grote aanslag plaatsvindt en de inlichtingendiensten zeggen, wij hadden die bevoegdheid moeten hebben, en we hebben het daardoor niet kunnen voorkomen, dan heeft de heer wilders heel veel uit te leggen.

Lubach: Wow, oke. Dus Segers zegt hier eigenlijk: als je kritiek hebt op de wiv, dan heb je bloed aan je handen. Oke, nou. Liegen, terreurschwalbes, maar de regering had nog een truc: Ze stuurde de huidige baas van de AIVD (...) naar Huys. AIVD directeur Rob Bertholee mocht aanschuiven bij college tour. Waarom wilde Twan Huys en zijn redactie heb zo graag te gast hebben? Nou, Twan Huys legt dat uit:

Fragment: Huys: “De AIVD heeft ons benaderd met de vraag of we interesse hadden. Dat komt zelden voor maar in dit geval heeft het te maken met de zogenaamde sleepwet.”

Lubach: Tuurlijk, het is campagnetijd. Bertholee nodigt gewoon zichzelf uit bij college tour. En hij mocht nog komen ook. Hoe kreeg hij dat voor elkaar?

Fragment: We hebben Bertholee laten weten dat hij niet alleen met feiten moest komen die we ook in het jaarverslag zouden kunnen vinden. Dan zou het niet doorgaan. Daar is de AIVD mee akkoord gegaan. Hij vertelde heel open en kwam met een aantal zaken die we niet wisten.

Lubach: Wat? Als er 1 iemand is waarvan je niet wil dat hij met primeurtjes komt, in een interviewprogrammatje, dan is het wel de baas van de AIVD. Óf informatie moet niet naar buiten komen en dan wil ik ook dat de AIVD er niks over zegtt, of het moet wel naar buiten komen en dan moeten ze het zo snel mogelijk zeggen. Maar Bertholee vertelde trots aan Huys dat hij 4 aanslagen had verijdeld. Dus blijkbaar heeft de AIVD ook nog een laatje met speciale geheimpjes om de pers mee te paaien voor als ze een referendum willen beinvloeden. (...) Nou, hoe ging dat interview bij college tour? (...) Bertholee zat dat natuurlijk vooral om tegenstanders van de nieuwe wiv te overtuigen. En dit was zijn boodschap aan mensen die tegen de wet zijn omdat er een paar onderdeeltjes niet deugen.

Fragment: Bertholee: “Je moet je realiseren dat als je tegen de wet bent, blijkbaar op grond van dat ene kleine deeltje (...) en dat je als het ware doormoddert met de oude wet.”

Lubach: Berholee doet alsof tegenstaders van deze nieuwe wet meteen helemaal geen nieuwe wet willen. En dat is niet zo. Niemand wil terug naar die vorige wet, want die was nog veel slechter. Het is alsof je tegen de ober zegt ‘mag ik een ander soort salami op de pizza’ en dat de over dan zegt ‘oh u wilt dus nooit meer eten’. (...) De voorstanders verzinnen dus de wildste verhalen over wat de tegenstanders willen. Dit is bijvoorbeeld VVD-kamerlid Malik Azmani, die heeft geen verhaal, die heeft een halve ridderroman.

Fragment: Azmani: “De VVD is natuurlijk voorstander van deze anti-terreurwet. We gaan toch ook niet, vraag ik aan u, militairen geridderd in harnassen op paarden met speren naar oorlogsgebied sturen? Terwijl we weten dat de tegenstanders daar met vol-automatische wapens, gevechtshelikopters, drones klaarstaan. Nee.”

Lubach: Nee. Maar dit zegt ook helemaal niemand. (...) Dit is het beeld wat de voorstanders van de  wiv schetsen van tegenstanders. Een stelletje onverantwoordelijke idioten die niets geven om veiligheid en terug willen naar de middeleeuwen. Maar dat is echt een smerige tactiek. Waar nu, voor eens en voor altijd (...) een eind aan moet komen. Laten we nog één keer kijken naar waar het meningsverschil nou wel om draait:
(...)


(...)
'Is de nieuwe wiv goed genoeg?' Hier pas ontstaat een meningsverschil. Hier heb je aan de ene kant Ollongren, Rutte (...) die zeggen 'Ja, die nieuwe wiv is prima, niks meer aan doen' en aan de andere kant heb je alle privacy organisaties, amnesty, de raad van state (...). En die zeggen 'Nee, de nieuwe wet moet op een paar punten nog worden aangepast. Dus hier gaat dit hele referendum over. Terwijl de regering dus doet alsof wij daar rechtsbovenin zitten. Alsof we gestoord zijn en zelfs gevaarlijk. Dus ik zeg, ga woensdag stemmen. Stem 'tegen' of 'nee' of 'blanco' of wat je maar wil. Maar lees er nog wat over, en kies wat jou goed lijkt. (...)

**Waar kan het misgaan met de zogenaamde sleepwet? 5 UUR LIVE**

Waar het in mijn ogen echt mis kan gaan is bij de zogenoemde hackbevoegdheid. De diensten hebben nu al een hackbevoegdheid, en ze krijgen er nu de bevoegdheid bij om ook derden te hacken. Je kan je voorstellen dat terroristen bijvoorbeeld heel veel maatregelen nemen om hun communicatie te versleutelen. Daar kom je niet zo makkelijk bij, dus die kan je ook niet zo makkelijk hacken.

Maar, bijvoorbeeld, journalisten die in contact staan met die terroristen omdat ze een verhaal over de jihad willen schrijven, die nemen niet die maatregelen. En de diensten mogen nu dus derden hacken om bij hun targets te komen.

En wat kan er dan gebeuren met zo'n journalist?

Daarvan kan dan de informatie in Zoetermeer komen te liggen. – Geldt bijvoorbeeld ook voor advocaten, die zijn bang dat de communicatie die zij met hun client hebben, die vertrouwelijk is, en al heel vaak geschonden wordt overigens, dat die ook in dat sleepnet worden meegenomen. En die zijn bang dat die niet meer op een vertrouwelijke manier met hun cliënten kunnen communiceren.

**Radar (AVROTROS)**

**Sleepnetwet: Bestaat privacy straks nog wel? (4:33), 25 september 2017**

(…)

Hertsenberg: Geheime diensten zoals de AIVD mogen vanaf 1 januari 2018 iedereen afluisteren, ook als er géén aanleiding is.

(…)

H: De bevoegdheden van de diensten worden flink uitgebreid. Zo mag er een zogenaamd sleepnet worden ingezet om massaal online communicatie af te luisteren, ook van niet-verdachte personen. Een hele wijk kan bijvoorbeeld worden afgeluisterd wanneer er één verdacht persoon in woont. Telefoons, computers, smart-tv's mogen gehackt worden. En er mag een geheimde DNA-databank worden aangelegd, waar iedereen in terecht kan komen. Verzamelde data mag met buitenlandse diensten gedeeld worden.

(…)

Aan tafel Eduard Nazarski, Amnesty International, en drie studenten (initiatiefnemers)

Student: "Dit gaat iedereen aan omdat het niet alleen gaat om de kattenplaatjes die je bekijkt op het internet. Het gaat ook om je medische gegevens, je locaties, je zoekopdrachten. Je privacy staat fundamenteel aan een heleboel rechten. Aan de persvrijheid, aan medische bescherming. En daarom gaat het iedere Nederlander aan. Het verschuift heel veel macht van de burger naar de staat."

H: waarom heeft Amnesty zich bij dit initiatief aangesloten?

Nazarski: (…) "Wij vinden dat die wet niet mensenrechtenproof is, die biedt niet genoeg waarborgen om mensenrechten te garanderen. Veiligheidsdiensten kunnen echt heel veel afluisteren, met dat sleepnet heel veel gegevens achterhalen, en dat is in strijd met mensenrechten en met privacy."

H: Maar een criticaster zou kunnen zeggen: als je niets te verbergen hebt dan is die wet ook geen probleem.

N: "Dat hoor ik wel vaker, en ik doe ook niets verkeerd denk ik, maar ik vind toch niet dat al mijn gegevens, alles wat ik doe, al mijn medische gegevens bijvoorbeeld, die hoeven niet overal op tafel te liggen. Wat ik wil bespreken, met mijn familie, met mijn vrienden, dat maak ik zelf wel uit, maar daar heb ik niemand voor nodig die dat voor mij gaat doen, die dat gaat verspreiden. En zo zijn er veel dingen waarvan je denkt, die zouden bij jezelf moeten blijven"

H: Maar is die wet niet nodig om terrorisme te verspreiden?

N: "Ja natuurlijk wil je terrorisme bestrijden, maar terroristen, die willen onze vrijheid aantasten. Wat we nodig hebben is een wet die terreur goed kan bestrijden, maar die niet onze vrijheden fundamenteel aantast. En door zo'n enorme sleepnetwet uit te vaardigen, door die diensten zoveel bevoegdheden te geven, *door niet te zorgen dat er rechterlijk toezicht vooraf*

*is, daardoor zijn er gewoon niet genoeg waarborgen*, en daardoor is het heel belangrijk dat die discussie ontstaat en dat die wet ook veranderd wordt.

H: Want de rechter is eigenlijk buitenspel gezet?

N: "*Die is buitenspel gezet. (…) Er is wel een commissie die alles moet toetsen maar die is lang niet zelfstandig genoeg.*

H: En is zo'n sleepnet nou eigenlijk effectief?

N: "Ik denk het niet. Ik denk dat heel veel andere deskundigen, zoals Beatrice de Graaf, die zeggen 'je moet terreur op een hele andere manier bestrijden. Je moet niet zo'n enorm sleepnet uitgooien en dan daarin onderzoek doen. Je moet op een heel andere manier terreur bestrijden.' (…) Wat Amnesty heel belangrijk vindt is dat er meer wordt nagedacht en gediscussieerd over waar deze wet precies voor dient en welke waarborgen je kunt inbouwen om onze privacy niet aan te tasten.

H: Dus als je recht op privacy je lief is dan is het heel belangrijk om deze actie te steunen.

N: Heel belangrijk.

**Buitenhof**

Axel Arnbak: Het belangrijkste bezwaar is eigenlijk dat het volslagen onduidelijk is hoe die bevoegdheid ingezet zal worden. Je kunt een debat voeren over of je wel of niet aan inlichtingendiensten de mogelijkheid verschaft om op grote schaal burgers af te luisteren. (…)

Of je het nou over privacy of over andere grondrechten hebt, dit is zo'n beetje de nuclear option. Als je deze in de wet vastlegt, is dat een beetje het schrikbeeld van een Big Brother die alles gaat afluisteren.

Witteman: En is dat terecht?

A: Toen de wet werd geïntroduceerd waren de wettelijke bepalingen heel erg onduidelijk, dus het schrikbeeld was toen zeker terecht. Naar mate de parlementaire behandeling vorderde zijn er hier en daar wat toezeggingen gedaan, maar nog steeds, en dat is ook een reden voor mij om tegen deze wet te pleiten, is het nog onvoldoende duidelijk voor mij hoe deze nuclear option ingezet gaat worden.

(…)

A: Het gaat erom dat in de wet de waarborgen voor het inzetten van dat middel ontoereikend zijn. (…) als je de parlementaire behandeling leest zegt de minister "geen wijk, dat gaan we niet doen", maar dat is helemaal niet waar. Dat hangt af van de doelstelling van het intercepteren van het verkeer.

(…) – over of de vergaande nieuwe bevoegdheden nodig zijn

A: Je kan, als er voldoende bewijs is, een debat voeren over de bepaalde bevoegdheden en sich. *Maar naar mate de bevoegdheid die je inzet zwaarder is, moeten daar veel strakkere waarborgen en veel beter toezicht tegenover staan*. (…)

Hoe kunnen we de rechter zover mogelijk op afstand zetten? We benoemen een commissie van drie wijzen, met twee oud-rechters en een cyber-expert, die dan toevallig ook oud-AIVD'er is (…).

W: Maar wat had U dan wel gewild?

A: Ik vraag me oprecht af waarom dat niet de rechtbank in Den Haag is geworden. (…)

Op dit punt wil ik één heel belangrijk punt maken. Het gaat er helemaal niet om of je de diensten nu vertrouwt, of je de overheid vertrouwt. Die waarborgen zijn er natuurlijk voor een situatie waarin de overheid niet meer te vertrouwen is, of buitenlandse diensten waarmee die informatie wordt gedeeld niet meer te vertrouwen zijn. 5 jaar geleden werd de rode loper hier op de gracht voor Vladimir Poetin uitgerold. (…) Erdogan hetzelfde verhaal, een kijk nu waar we staan. Een rechter is beter geëquipeerd om als zoiets zich in Nederland voltrekt om daar een onafhankelijk en bindend oordeel over te vellen.

Het gaat er dus niet om of onze diensten wel of niet goed werk verrichten, het gaat erom dat er een situatie kan ontstaan waarin alles misschien anders gaat. Dat is een essentieel argument.

(…)

Een ander punt is de bewaartermijn van drie jaar. Stel een set data wordt gedeeld met een buitenlandse dienst, denk nou niet dat die rekening gaan houden met deze bewaartermijn. Ook daar zit een belangrijke achilleshiel van deze wet. Mevrouw Aerts zegt dat een eventueel ander regime zich niet aan deze wet zal houden, maar met deze wet kunnen we nog altijd naar het EHRM of naar Luxemburg (EHJ). Daarom is het cruciaal dat we dit in deze wet hebben staan.

**EenVandaag**

(…) Wie goed kijkt vandaag ziet niet één, maar ook nog een tweede stemdoos. Ook nog ééntje voor het referendum. We kunnen ons uitspreken voor of tegen de aftapwet, de wet op de inlichtingen- en veiligheidsdiensten. De initiatiefnemers van het referendum voerden vandaag nog campagne.

"Stem vandaag op het referendum tegen de sleepwet. Tegen het massaal afluisteren van burgers"

(…)

5 studenten filosofie, neurowetenschappen, en logica. Ze bedenken zeven maanden geleden dat de nieuwe wet op de inlichtingen- en veiligheidsdiensten een onding is.

"Het is niet voor niets te privacy een mensenrecht is, dat is er om jou juist veilig te houden tegen de overheid, en zodra dat recht wordt geschonden zijn wij eigenlijk allemaal onveiliger."

**Nieuwsuur**

Willem Spaans (voorzitter Burgercomité Nederland)

"Wat mij tegenstaat is het feit dat de overheid toegang heeft tot allerlei informatie, over willekeurige, en veelal goedwillende en onschuldige burgers, waar ze eigenlijk niets mee te maken hebben."

Dennis Broeders (WRR): "In de zomer is de wet in de Eerste Kamer doorgestemd, en daarmee is de wet een feit."

Nieuwsuur: En hoe belangrijk is het voor de MIVD en de AIVD dat deze wet doorgaat?

B: "Nou het is heel belangrijk, die wet was echt gedateerd."

(…)

Nieuwsuur: Onder de nieuwe wet mogen de diensten op grote schaal informatie van internet verzamelen. Een voorbeeld: In een Haagse wijk woont een verdacht persoon die mogelijk een aanslag voorbereidt. Om erachter te komen of hij met iemand samenwerkt mogen de diensten internetverkeer van iedereen in de buurt aftappen. Denk aan de straat, wijk of omgeving."

B: "Ik kan me voorstellen dat de Belgische diensten wellicht de zaak hebben gemaakt van kunnen we niet heel Molenbeek voor een periode tappen. Dan tap je ook iedereen af die daar gewoon z'n normale leven leidt en gewoon z'n gang gaat. En dan komt dus de grote vraag van 'is dat proportioneel?'".

N: Tegenstanders vrezen dat mensen ten onrechte als verdachte komen bovendrijven op basis van verkeerde computerberekeningen.

B: "Ja dat kan, of je daarmee geconfronteerd wordt is nog een tweede. Heel veel van dit soort analyses zullen ook een leven leiden in de backoffices maar misschien later nog een keer opkomen, maar we weten dat niet precies. Daarom is het ook zo belangrijk dat een toezichthouder namens ons kijk van 'hoe gaat dat dan?'"

N: Wie houdt in de gaten of de veiligheidsdiensten zich aan de wet houden? De AIVD en de MIVD mogen niet zomaar tappen op internet. Om op grote schaal informatie te mogen verzamelen moeten de diensten eerst toestemming vragen aan de minister van BZK. Als de minister zijn fiat geeft controleert een speciale commissie van oud-rechters of die toestemming terecht gegeven is. Zo ja, dan mogen de data verzameld en geanalyseerd worden. Aan het einde van de rit controleert de CTIVD of alles volgens de regels is gegaan.

*Er is veel kritiek op de commissie die te toestemming moet geven. Het zou een stempelmachine worden. De Raad van State heeft het zelfs over een alibi-functie.*

B: Als de RvS dat zegt dan zou ik als onafhankelijk expert in die toetsingscommissie dat als een grote aansporing. Die toetsingscommissie moet zich wat dat betreft ook bewijzen.

S: *"Als dat door een commissie eerst gecontroleerd moet worden, op papier is dat allemaal leuk, in de werkelijkheid weten we dat dat niet werkt. Want op het moment dat één kamerlid of één minister zegt 'terrorisme' dan zal die commissie zeggen: 'ja, het is gerechtvaardigd om ernaar te gaan kijken."*

N: Bij de CTIVD, de toezichthouder die achteraf kijkt of de diensten zich aan de wet hebben gehouden, werken maar 12 onderzoekers.

B: "*Het contrast met de diensten zelf is vrij groot, dat is wat dat betreft echt David en Goliath. (…) Ik denk wet, gezien wat we nu optuigen, een ook wat we in andere landen hebben gezien, we hebben natuurlijk de Snowden-onthullingen gezien, dat is van een totaal andere orde dan wat we hier zien. Maar toch, we bewegen toch wel in een richting waarin we steeds meer datagedreven gaan werken, dan moeten we ook een datageoriënteerde toezichthouder hebben die daar daarwerkelijk toezicht op kan hebben*.

N: En is dat nu in proportie?

B: "*Ik zou dat graag wat versterkt zien*"

**Het debat over de sleepwet (23:30), 5 maart 2018**
**https://radar.avrotros.nl/uitzendingen/gemist/item/het-debat-over-de-sleepwet/**

(…)

Hertsenberg: Goed, Quirine Eijkman, bent u bang dat deze wet gevolgen heeft voor de privacy van burgers?

Eijkman: Nou dat heeft deze wet zeker, het heeft een behoorlijke inbreuk op de privacy, en dat mag ook. Want we hebben niet voor niks een inlichtingendienst die onze veiligheid beschermt, dat is dus

ook een mensenrecht. Tegelijkertijd is de inbreuk vrij fors. *En dat klopt dat er waarborgen zijn, de vraag is of die waarborgen toereikend zijn*. En niet te veel gefocust zijn alleen op de wet, maar ook of het doel, de doelmatigheid goed is. Of het doel van de inzet van een bevoegdheid ook tot meer veiligheid leidt. Dat is één ding. Het tweede is de privacy van burgers die geen target zijn. Zeg maar niet mensen waar de AIVD misschien extra interesse in heeft. En dat kan je wel zien als een behoorlijke inbreuk.

H: Ja want daar worden ook gegevens van verzameld?

E: Ja, daar worden gegevens van verzameld. Nu wordt er wel een onderscheid gemaakt, ook in de controle. Vaak wordt er gezegd nou 98% van die gegevens wordt weggegooid. Dus de bulk wordt eigenlijk weggegooid. Maar je zou kunnen zeggen dat is toch ook een privacy inbreuk en bijvoorbeeld hoelang die gegevens wel of niet bewaard kunnen worden, daar zijn wel veel vragen over. Niet alleen door het College van de Rechten van de Mens maar ook door andere stakeholders.

H: Wat voor stakeholders heb je het dan over?

E: Je zag in het filmpje al, Bits for Freedom, 29 wetenschappers die gereageerd hebben, 1100 mensen die gereageerd hebben op de publieke consultatie van deze wet voordat die naar de Tweede Kamer ging. Daar is iets mee gedaan, in het tweede wetsvoorstel. Maar je had nog veel beter kunnen luisteren naar de vijftig amendementen en moties die in de Kamer zijn besproken. En bijna geen enkele is daarvan aangenomen.

(…)

H: Bent u het eens dat het op deze wet beter is dan elders in Europa?

E: *Nou, op onderdelen misschien zeker, op andere onderdelen niet. Maar we hebben ook wel hele ruime bevoegdheden op deze wet. En dan hebben we gezegd: ''Vooraf is er een rechtmatigheidstoets. Dus klopt het wat er in de wet staat?'' Achteraf hebben we ook toezicht, van die controlecommissie de CTIVD. Commissie van toezicht, alleen dat is niet altijd bindend. We hebben ook nog de Tweede Kamer, er wordt weleens gezegd: ''De commissie stiekem, de vijf belangrijkste fractievoorzitters in de Tweede Kamer. Daar is heel veel toezicht''*. Maar er worden ook hele ruime bevoegdheden gecreëerd. En de vraag is of je dat niet bindend moet laten zijn. De bewaartermen van die data waar ik het eerder over had, zijn ook vrij fors

(…)

H: Ja, mevrouw Eijkman, wat denkt u? Is de wet tekstgericht genoeg? En duidelijk genoeg?

E: Nou, het is op zich ingewikkelde materie, maar dat komt ook omdat er heel veel verschillende bevoegdheden in staan. Het is zeker nodig, dat stellen het College voor de Rechten van de Mens en anderen ook niet ter discussie. Maar de vraag is: ''Hoe breed zijn die bevoegdheden''? En de commissie Dessens, die heeft zeg maar het vooronderzoek gedaan van deze wet, zij zeiden: '*'Het is absoluut nodig, de technologie, maar daar moet forse controle tegenover staan''*. Niet alleen of het mag in de wet, maar ook of het doelmatig is, dus wordt dat doel bereikt? En daar kan je wel vragen over stellen. Dat is besproken in de Eerste Kamer, maar ook in de Tweede Kamer. Tegelijkertijd kan je zeggen: ''Nou, hoe hard is die garantie''? Professor van Eijk zei het net ook, hopelijk wordt het meegenomen in de evaluatie over twee jaar, maar dat zijn geen harde toezeggingen.

Bertholee (AIVD): Het zit wel in de wet he, de doelbinding. Een van de, elke keer als we een bijzondere bevoegdheid toepassen, als we, laat ik het maar even noemen, als we tappen, of hacken of iets anders doen. Elke keer opnieuw, dan moeten wij ons afvragen voordat we dat doen, past het in het onderzoek wat we opgedragen gekregen hebben?

H: U mag dat niet zomaar doen?

B: Ik mag het niet zomaar doen.

H: Nee.

B: Ik moet afwegen of het proportioneel is, of de inbreuk op de privacy in verhouding staat tot het plan dat gediend is en of het echt het lichtste middel is wat beschikbaar is.

H: Ik hoor een maar

E: Ja dat is zeker zo, en dat doet de dienst nu ook al. Tegelijkertijd zou je kunnen zeggen voor het vertrouwen van mensen die ook gaan stemmen in dit referendum, is het goed om te horen dat de diensten dat doen en dat deden ze ook al. Tegelijkertijd, in hoeverre is de controle daarop he, of het proportioneel gebeurt of niet, in hoeverre is dat voldoende? Nou die toezegging…

H: Proportioneel is, hoe smal is dan ook de groep die onderzocht wordt? Bedoelt u dat met proportioneel?

E: Ja, nou je zou ook kunnen zeggen van, het middel, is dit nou het doel wat we proberen te bereiken, ik zeg maar wat dat iemand wil uit racen, kan dat ook met het lichtst mogelijke middel bereikt worden? En die afweging die wordt gemaakt, daar heeft u heel veel, en uw mensen heel veel ervaring mee. Maar de vraag is, wordt dat ook door de toezichtscommissies zo gezien en de rest van Nederland? Volgens mij gaat daar deels het debat over, over de legitimeit, het vertrouwen dat het goed gebeurt. En dat is er misschien op dit moment wel. Maar we leven ook in onrustige tijden, er kan een andere regering komen, etc. Daar zijn gewoon wel vragen over.

(…)

H: Ja, wat is het bezwaar van het verzamelen van metadata?

E: Nou, daar is op zich geen bezwaar tegen. Maar de vraag is in hoeverre maak je een inbreuk op privacy? En ik denk net dat de directeur van Bits of Freedom, zegt van: Nou ja, het is wel iets minder onschuldig dan alleen of het een rode Toyota is ofniet die is in die snelweg. Maar het gaat er eigenlijk om: ‘’In hoeverre zien we nou dat er nou echt een inbreuk is op de privacy’’. En dat is eigenlijk, denk ik, het meest belangrijke. Dat wordt op zich ook wel geregeld in de wet met die toets waar we het net over hadden. Maar de vraag is weer, hoeveel metadata mag je…

H: Mag je bewaren. Het mag drie jaar bewaard blijven?

(…)

E: Het feit zeg maar dat in de wet wordt geregeld, is niet een soort cadeautje ofzo. Er is ook privacy- en data protectiewetgeving waar wij ons ook aan te houden hebben. Sterker nog, er zijn al mensen die willen gaan procederen over een vrij forse bewaartermijn van drie jaar. En in andere landen wordt daar wel wisselend over gedacht. Bijvoorbeeld, Duitsland maakt wel echt een verschil tussen binnen- en buitenland. En zeker voor de binnenlandse data, zijn er andere regels geldig. Dus dat is bijvoorbeeld een voorbeeld waar Nederland wel afwijkt.

(…)

E: Nou, opzich zijn die waarborgen goed, en daar is ook een toets helemaal ingebouwd zodat er ook onder anderen naar mensenrechten wordt gekeken. Maar die toets is vrij generiek.

H: Heel algemeen

E: Een beetje algemeen, en tegelijkertijd gaat het als het om bulkdata gaat, is het weer een hele hoop data. Dus niet van één specifiek persoon of een specifieke schijf. Je zou kunnen zeggen misschien moet de controle daarop verscherpt worden. Nou daar is ook veel discussie over en ik denk ook zeker dat het over twee jaar in die evaluatie aan bod gaat komen, als er namelijk op één punt veel kritiek is, dan is het dit punt, dat delen van ongeëvalueerde gegevens inderdaad.

H: Het zou dan kunnen zijn dat er dan gegevens gedeeld worden, waarvan later in Nederland, na analyse gezegd wordt, die hadden we eigenlijk niet kunnen geven. Zou dat kunnen?

E: Dat is misschien een mogelijkheid, kijk ik deel wel wat u zegt, dat wordt niet zomaar gedaan. En daar is ook door die CTIVD, die commissie van toezicht, zijn er best wel een aantal rapporten over geschreven. Maargoed, het staat wel in de wet en het is wel mogelijk. Nogmaals, we kunnen ook wel op termijn met landen zaken gaan doen waarvan we zeggen: ‘’Ja, dat hadden we toch niet willen doen’’

**Roel Maalderink – Dit doen mensen stiekem op hun telefoon / Sleepwet (3:17, 83K), 5 oktober 2017 https://www.youtube.com/watch?v=qIpM2bz23ak**

Niks te verbergen? Vanaf 1 januari treedt de Sleepwet (WiV) in werking, die het massaal aftappen van online communicatie mogelijk maakt. Tenzij men tekent voor het referendum tegen dat Sleepnet. Is men tegen die sleepwet of heeft men niks te verbergen? En wat nou als je - net als de overheid - door de gegevens van die mensen gaat? Hebben ze dan nog steeds niks te verbergen?

Er mag een zogenaamd “sleepnet” worden ingezet om massaal online communicatie af te luisteren, ook van niet verdachte burgers. Zo mag een hele wijk afgeluisterd worden wanneer er een verdacht persoon in woont. Alle geautomatiseerde apparaten mogen gehackt worden. Denk bijvoorbeeld aan uw telefoon, computer of smart-tv. Er mag een geheime DNA-databank aangelegd worden waar iedereen in terecht kan komen. Verzamelde data mag met buitenlandse inlichtingendiensten gedeeld worden, ook zonder deze eerst geanalyseerd te hebben."

(…)

Maalderink: Mag ik ook in de foto’s kijken, even?

Passant: “Nou, liever niet eigenlijk”

M: Hoezo niet?

P: “Omdat dat iets tussen ons tweeën is eigenlijk…” “Ik vind het niet zo fijn dat je hier nou inkijkt”

M: Nee?

P: “Nee”

M: Maar dat gaan ambtenaren binnenkort dus ook doen.

P: “Oke”

M: Als er iemand in de buurt woont die een misdrijf heeft gepleegd dan mogen ze ook jouw internetverkeer aftappen.

P: “Oh”

M: Maar… Je kan nu een handtekening indienen voor een referendum over die wet, de sleepwet, en als er 300.000 handtekeningen zijn dan komt er een referendum over.

P: “Waar kan ik dat indienen?”

M: Dat kan op teken.sleepwet.nl